

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Masami NASU

SERIAL NO: 10/810,696

FILED: March 29, 2004

FOR: COMMUNICATION DEVICE, SOFTWARE UPDATE DEVICE, SOFTWARE UPDATE SYSTEM,
SOFTWARE UPDATE METHOD, AND PROGRAM

GAU: 2122

EXAMINER:

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number _____, filed _____, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. Date Filed

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:


<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2003-090827	March 28, 2003
JAPAN	2003-090886	March 28, 2003
JAPAN	2004-058270	March 2, 2004
JAPAN	2004-058271	March 2, 2004

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. _____ filed _____
- ☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. _____ filed _____; and
- ☐ (B) Application Serial No.(s)
☐ are submitted herewith
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Marvin J. Spivak
Registration No. 24,913

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

Joseph A. Scafetta, Jr.
Registration No. 26, 803

101810, 696

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日 2003年 3月28日
Date of Application:

出願番号 特願2003-090827
Application Number:

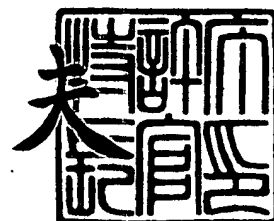
[ST. 10/C]: [JP2003-090827]

願人 株式会社リコー
Applicant(s):

2004年 2月 4日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

CERTIFIED COPY OF
PRIORITY DOCUMENT

出証番号 出証特2004-3005867

【書類名】 特許願

【整理番号】 0302157

【提出日】 平成15年 3月28日

【あて先】 特許庁長官 殿

【国際特許分類】 G03G 21/00 396

【発明の名称】 ファームウェア更新装置、ファームウェア更新システム
、ファームウェア更新方法及びプログラム

【請求項の数】 19

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

【氏名】 奈須 政巳

【特許出願人】

【識別番号】 000006747

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号

【氏名又は名称】 株式会社リコー

【代表者】 桜井 正光

【代理人】

【識別番号】 100080931

【住所又は居所】 東京都豊島区東池袋 1 丁目 2 0 番 2 号 池袋ホワイトハ
ウスビル 8 1 8 号

【弁理士】

【氏名又は名称】 大澤 敬

【手数料の表示】

【予納台帳番号】 014498

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809113

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ファームウェア更新装置、ファームウェア更新システム、ファームウェア更新方法及びプログラム

【特許請求の範囲】

【請求項 1】 ネットワークを介して被更新装置と通信可能なファームウェア更新装置であって、

前記被更新装置のファームウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第 1 の通信経路で前記被更新装置に送信して記憶するよう要求する認証情報設定手段と、

前記被更新装置に前記更新用認証情報を前記第 1 の通信経路よりも処理負荷の小さい第 2 の通信経路で送信し、該認証情報による認証処理を要求する認証要求手段と、

該認証処理が成功した場合に更新用ファームウェアを前記第 2 の通信経路で前記被更新装置に送信する送信手段とを設けたことを特徴とするファームウェア更新装置。

【請求項 2】 請求項 1 記載のファームウェア更新装置であって、

前記更新用ファームウェアの送信後に、前記被更新装置に対して前記更新用認証情報の無効化要求を送信する認証情報無効化手段を設けたことを特徴とするファームウェア更新装置。

【請求項 3】 請求項 1 又は 2 記載のファームウェア更新装置であって、

前記被更新装置のファームウェアの更新を、外部からのファームウェア更新要求に応じて行い、その結果を該更新要求の要求元に返す手段を設けたことを特徴とするファームウェア更新装置。

【請求項 4】 請求項 1 乃至 3 のいずれか一項記載のファームウェア更新装置であって、

前記被更新装置から起動した旨を示す起動通知を受け付ける手段と、

前記更新用ファームウェアの送信後に前記被更新装置から前記起動通知を受け付けた場合に該被更新装置からファームウェアのバージョン情報を取得し、送信した更新用ファームウェアのバージョン情報と比較して更新の成否を確認する手

段とを設けたことを特徴とするファームウェア更新装置。

【請求項5】 請求項1乃至4のいずれか一項記載のファームウェア更新装置であって、

前記第1の通信経路はSSLによる通信を行う通信経路であり、

前記第2の通信経路はFTPによる通信を行う通信経路であることを特徴とするファームウェア更新装置。

【請求項6】 ネットワークを介して互いに通信可能なファームウェア更新装置と被更新装置とによって構成されるファームウェア更新システムであって、

前記ファームウェア更新装置に、

前記被更新装置のファームウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第1の通信経路で前記被更新装置に送信して記憶するよう要求する認証情報設定手段と、

前記被更新装置に前記更新用認証情報を前記第1の通信経路よりも処理負荷の小さい第2の通信経路で送信し、該認証情報による認証処理を要求する認証要求手段と、

該認証処理が成功した場合に更新用ファームウェアを前記第2の通信経路で前記被更新装置に送信する送信手段とを設け、

前記被更新装置に、

前記更新用認証情報を記憶するよう要求された場合にこれを記憶する記憶手段と、

前記認証処理を要求された場合に、受信した更新用認証情報と前記記憶手段に記憶している更新用認証情報とを用いて認証処理を行って結果を返す認証手段と、

該認証処理が成功した場合に前記更新用ファームウェアを受信し、自機のファームウェアを該更新用ファームウェアに更新する更新手段とを設けたことを特徴とするファームウェア更新システム。

【請求項7】 請求項6記載のファームウェア更新システムであって、

前記ファームウェア更新装置に、

前記更新用ファームウェアの送信後に、前記被更新装置に対して前記更新用認

証情報の無効化要求を送信する認証情報無効化手段を設け、

前記被更新装置に、

該無効化要求を受信した場合に前記記憶手段に記憶している更新用認証情報を無効化する手段を設けたことを特徴とするファームウェア更新システム。

【請求項 8】 請求項 6 又は 7 記載のファームウェア更新システムであって、

前記被更新装置に、

前記更新手段によるファームウェアの更新後に自機を再起動する手段と、

起動時に前記ファームウェア更新装置にその旨を示す起動通知を送信する手段と、

前記ファームウェア更新装置からの要求に応じて該装置にファームウェアのバージョン情報を送信する手段とを設け、

前記ファームウェア更新装置に、

前記更新用ファームウェアの送信後に前記被更新装置から前記起動通知を受け付けた場合に該被更新装置に対してファームウェアのバージョン情報の送信を要求して該バージョン情報を取得し、送信した更新用ファームウェアのバージョン情報と比較して更新の成否を確認する手段を設けたことを特徴とするファームウェア更新システム。

【請求項 9】 請求項 6 乃至 8 のいずれか一項記載のファームウェア更新システムであって、

前記第 1 の通信経路は SSL による通信を行う通信経路であり、

前記第 2 の通信経路は FTP による通信を行う通信経路であることを特徴とするファームウェア更新システム。

【請求項 10】 ファームウェア更新装置によって、ネットワークを介して通信可能な被更新装置のファームウェアを更新するファームウェア更新方法であって、

前記被更新装置のファームウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第 1 の通信経路で前記被更新装置に送信して記憶させ、

前記被更新装置に前記更新用認証情報を前記第 1 の通信経路よりも処理負荷の

小さい第2の通信経路で送信して該認証情報による認証処理を行わせ、

該認証処理が成功した場合に更新用ファームウェアを前記第2の通信経路で前記被更新装置に送信してファームウェアの更新を行わせることを特徴とするファームウェア更新方法。

【請求項11】 請求項10記載のファームウェア更新方法であって、

前記更新用ファームウェアの送信後に、前記被更新装置に前記更新用認証情報を無効化させることを特徴とするファームウェア更新方法。

【請求項12】 請求項10又は11記載のファームウェア更新方法であって、

前記被更新装置のファームウェアの更新を、外部からのファームウェア更新要求に応じて行い、その結果を該更新要求の要求元に返すことを特徴とするファームウェア更新方法。

【請求項13】 請求項10乃至12のいずれか一項記載のファームウェア更新方法であって、

前記被更新装置から起動した旨を示す起動通知を受け付け、

前記更新用ファームウェアの送信後に前記被更新装置から前記起動通知を受け付けた場合に該被更新装置からファームウェアのバージョン情報を取得し、送信した更新用ファームウェアのバージョン情報と比較して更新の成否を確認することを特徴とするファームウェア更新方法。

【請求項14】 請求項10乃至13のいずれか一項記載のファームウェア更新方法であって、

前記第1の通信経路はSSLによる通信を行う通信経路であり、

前記第2の通信経路はFTPによる通信を行う通信経路であることを特徴とするファームウェア更新方法。

【請求項15】 ネットワークを介して被更新装置と通信可能なファームウェア更新装置を制御するコンピュータを、

前記被更新装置のファームウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第1の通信経路で前記被更新装置に送信して記憶するよう要求する認証情報設定手段と、

前記被更新装置に前記更新用認証情報を前記第 1 の通信経路よりも処理負荷の小さい第 2 の通信経路で送信し、該認証情報による認証処理を要求する認証要求手段と、

該認証処理が成功した場合に更新用ファームウェアを前記第 2 の通信経路で前記被更新装置に送信する送信手段として機能させるためのプログラム。

【請求項 16】 請求項 15 記載のプログラムであって、

前記コンピュータを、前記更新用ファームウェアの送信後に、前記被更新装置に対して前記更新用認証情報の無効化要求を送信する認証情報無効化手段として機能させるためのプログラムをさらに含むことを特徴とするプログラム。

【請求項 17】 請求項 15 又は 16 記載のプログラムであって、

前記コンピュータを、前記被更新装置のファームウェアの更新を外部からのファームウェア更新要求に応じて行い、その結果を該更新要求の要求元に返す手段として機能させるためのプログラムをさらに含むことを特徴とするプログラム。

【請求項 18】 請求項 15 乃至 17 のいずれか一項記載のプログラムであって、

前記コンピュータを、

前記被更新装置から起動した旨を示す起動通知を受け付ける手段と、

前記更新用ファームウェアの送信後に前記被更新装置から前記起動通知を受け付けた場合に該被更新装置からファームウェアのバージョン情報を取得し、送信した更新用ファームウェアのバージョン情報と比較して更新の成否を確認する手段として機能させるためのプログラムをさらに含むことを特徴とするプログラム。

【請求項 19】 請求項 15 乃至 18 のいずれか一項記載のプログラムであって、

前記第 1 の通信経路は SSL による通信を行う通信経路であり、

前記第 2 の通信経路は FTP による通信を行う通信経路であることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、ネットワークを介して通信可能な被更新装置のファームウェアを更新するファームウェア更新装置、このようなファームウェア更新装置と被更新装置とによって構成されるファームウェア更新システム、上記のファームウェア更新装置によるファームウェア更新方法、コンピュータを上記のファームウェア更新装置として機能させるためのプログラムに関する。

【0002】**【従来の技術】**

従来から、プリンタ、FAX装置、コピー機、スキャナ、デジタル複合機等の画像処理装置において、ハードウェアの基本的な制御を行うためのソフトウェアであるファームウェアを更新可能とすることが行われている。そして、特許文献1には、サービスセンタが画像形成装置からファームウェアのバージョン情報を取得し、バージョンが古く、更新が必要だと判断した場合に通信コントロール装置を介して画像形成装置にファームウェアを送信してファームウェアの更新を行わせる画像形成装置管理システムが記載されている。

【0003】**【特許文献1】**

特開2002-288066号公報

【0004】

ところで、特許文献1に記載の画像形成装置管理システムは、基本的にサービスセンタと通信コントロール装置との間の通信は公衆回線（PSTN）や専用回線、通信コントロール装置と画像形成装置との間の通信はRS-485規格の通信経路を用いて行うものである。

これに対し、近年では、汎用性や拡張性を重視し、管理装置と被管理装置との間の通信を、インターネットやローカルエリアネットワーク（LAN）等のネットワークを介して行う管理システムが提案されている。そして、このような管理システムにおいても、特許文献1の場合と同様に、管理装置から被管理装置にファームウェアを送信してファームウェアの更新を行わせることが考えられる。

【0005】

この場合の処理として考えられるのは、例えば図 21 のシーケンス図に示す処理である。なお、この場合においては、管理装置はファームウェア更新装置（ファーム更新装置）、被管理装置はファームウェア（以下単に「ファーム」ともいう）の被更新装置であると考えられる。

図 21 に示す処理においては、ファーム更新装置 91 と被更新装置 92 とは F T P（File Transfer Protocol）を用いて通信を行うが、予めファーム更新装置 91 に F T P のための I D とパスワードを設定しておき、これらをファーム更新装置 91 と被更新装置 92 の双方に記憶させておくものとする。

【0006】

この処理において、まずファーム更新装置 91 が、一定時間毎あるいは所定のイベントが発生した場合等に、バージョン情報取得処理を実行し、被更新装置 92 に I D とパスワードを送信して F T P による接続を要求する。I D とパスワードは F T P の規格に従ったものであり、接続を要求された被更新装置 92 はこれらによってファーム更新装置 91 を認証することができる。そして、この I D とパスワードを記憶しているものと比較し、一致すれば認証成功として接続を確立する（S11）。I D 又はパスワードが一致しなかった場合には接続は確立されず、エラーとなって処理は終了する。

接続が確立されると、ファーム更新装置 91 は被更新装置 92 にファームウェアのバージョン情報を送信するよう要求し、被更新装置 92 がこれに応答してファームのバージョン情報を送信する（S12）。その後、ファーム更新装置 91 は被更新装置 92 との接続を切断する（S13）。以上がバージョン情報取得処理である。

【0007】

次に、ファーム更新装置 91 は取得したファームのバージョン情報をもとに更新の可否を判断する。既に最新のバージョンのファームが被更新装置 92 にインストールされていれば、更新は不要である。ここで更新不要と判断すれば処理を終了し、その後トリガが発生した場合に再度バージョン情報取得処理を行うことになる。しかし、更新が必要と判断すれば（S14）、次のファーム送信処理を実行する。

この処理では、まずステップ S 1 1 の場合と同様に被更新装置 9 2 に I D とパスワードを送信し、接続を確立する (S 1 5)。そして、更新用のファームを被更新装置 9 2 に送信する (S 1 6)。被更新装置 9 2 側では、これを受信すると、ファームの更新処理を行い (S 1 7)、更新が完了すると自身をリセットし、再起動して新たなファームを有効にする (S 1 8)。また、被更新装置 9 2 のリセットにより、F T P 接続は切断される。以上がファーム送信処理である。

以上の処理によって、必要な場合に被更新装置 9 2 のファームを更新することができる。そして、再度バージョン情報取得処理やファーム送信処理を行う場合も、シーケンス図の続きに同じステップ番号で示したように、同じパスワードを用いて同様な処理を行う。

【0008】

【発明が解決しようとする課題】

しかし、F T P による通信は、データを暗号化しないため、I D やパスワードも平文のままネットワーク上を転送されることになる。従って、図 2 2 に示すように、ファーム更新装置 9 1 と被更新装置 9 2 との間の通信経路をパケットモニタ 9 3 によってモニタリングすれば、転送されるデータパケットから I D やパスワードを取り出すことができてしまう。そして、これを悪用すれば、第 3 者がファーム更新装置 9 1 になりすまして被更新装置 9 2 にアクセスし、ファームを不正なものに更新させることも可能になってしまう。

従って、図 2 1 に示したように F T P によって送信したパスワードを何度も繰り返して用いることは、安全面で問題があると言える。

【0009】

なお、特許文献 1 に記載のように P S T N、専用回線、R S - 4 8 5 のような通信経路を用いた場合には、独自の通信プロトコルを用いて通信することになるため、各装置をハード的に解析し、プロトコルを知得しなければ通信をモニタリングすることができない。従って、モニタリングが困難であるので、このような安全面の問題は発生せず、そのためこの問題を解決する手段についても特に記載されていない。

しかし、T C P / I P (Transmission Control Protocol/Internet Protocol

）等のインターネットの標準技術を利用してファームウェア更新システムを構築しようとする場合には、このような安全面の問題の解決は重要な課題となる。

【0010】

ところで、上記の問題を解消するためには、通信内容を暗号化する通信プロトコルとして例えばSSL（Secure Socket Layer）と呼ばれるプロトコルが開発されており、広く用いられている。このプロトコルを用いて通信を行うことにより、公開鍵暗号方式と共通鍵暗号方式とを組み合わせ、通信相手の認証を行うと共に、情報の暗号化により改竄及び盗聴の防止を図ることができる。

このようなSSLによる通信を行えば、ファーム更新装置91と被更新装置92とが安全に共通鍵を交換することができ、通信を安全に行うことができる。しかしながら、SSLのように暗号化処理を含む通信方式は、認証やデータ転送に係る処理負荷が、FTPのように暗号化を行わない通信方式よりも大きくなってしまう。

【0011】

一方で、ファームウェアはハードウェアの基本的な制御を行うためのソフトウェアを含むため、ファームウェア自身に更新機能を設けた場合、更新に失敗すると装置が全く動作しなくなる恐れがある。そこで、このような事態を避けるため、更新処理用の更新プログラムを別途用意し、これ以外の部分のみのファームウェアを更新するようにしている。

そして、このようにした場合、ファームウェア更新時以外の通常動作時に使用しない更新プログラムのために大きな記憶容量を使用することは、コスト面等を考慮すると妥当でない。従って、更新プログラムはできるだけ容量が小さいものが好ましいという要求がある。

このような観点からは、上述のようにSSLを用いてファームウェアの更新を行うことは、更新プログラムの容量増加につながり、好ましくないとと言える。

【0012】

ところで、図21に示した処理の安全性を向上させる手段としては、通信を暗号化するほか、図23に示すようなパスワードリストを用いることも考えられる。

。

このパスワードリストは、ファーム更新装置 9 1 に設定された I D と対応するパスワードを多数生成し、順序をつけたものである。このようなパスワードリストは、メモリカード等に記憶させて書留郵便のようなネットワーク以外の安全な経路でファーム更新装置 9 1 と被更新装置 9 2 の管理者に送付し、それぞれの管理者が装置の記憶手段に記憶させておく。そして、ファーム更新装置 9 1 から被更新装置 9 2 に認証を要求する際には未使用のパスワードの中から先頭のものを選んで使用するようにし、使用したものは使用済みとして、次に認証を要求する際には次のパスワードを用いるようにするのである。

【0013】

このようなパスワードリストを用いる場合の図 2 1 と対応する処理は、例えば図 2 4 のシーケンス図に示すようになる。

図 2 4 に示す処理においても、ファーム更新装置 9 1 と被更新装置 9 2 とは F T P (File Transfer Protocol) を用いて通信を行う。

この処理においても、所定のイベントが発生した場合等にファーム更新装置 9 1 が被更新装置 9 2 に I D とパスワードを送信して F T P による接続を要求するが、その前にパスワードリストを参照して使用するパスワードを決定する (S 1 1)。ここでは、まだパスワードは 1 つも使用されておらず、先頭のパスワード A を選択するものとする。

【0014】

そしてその後、ファーム更新装置 9 1 は図 2 1 のステップ S 1 1 乃至 S 1 3 の場合と同様にバージョン情報取得処理を行って被更新装置 9 2 のファームのバージョン情報を取得する (S 4 2 ~ S 4 4) が、この際に用いるパスワードはステップ S 1 1 で選択したパスワード A である。そして、被更新装置 9 2 も同じパスワードリストを記憶しているので、これを参照して先頭のパスワード A と比較することにより、認証処理を行うことができる。

バージョン情報取得処理が終了すると、ファーム更新装置 9 1 はパスワード更新処理を開始し、H T T P (Hyper Text Transfer Protocol) を用いて被更新装置 9 2 にパスワード更新要求を送信する (S 4 5)。そして、この要求に従って、被更新装置 9 2 はパスワードリストのうちの使用したパスワード (パスワード

A) を使用済みに設定し (S 4 6)、これが成功すると更新 OK 通知を返す (S 4 7)。

【0015】

ファーム更新装置 9 1 は、この通知を受け取ると、被更新装置 9 2 と同じように、使用したパスワードを使用済みに設定する (S 4 8)。以上がパスワード更新処理であり、この処理によって、ファーム更新装置 9 1 と被更新装置 9 2 の双方で、一度 F T P で転送したパスワードを使用済みとし、まだ使用していない次の安全なパスワード (パスワード B) を使用するように設定することができる。ただし、続けてファーム送信処理を行う場合には、ファーム送信処理の終了まではバージョン情報取得処理で用いたパスワードをそのまま使用するものとする。

【0016】

次に、ファーム更新装置 9 1 はステップ S 4 3 で取得したファームのバージョン情報をもとに更新の要否を判断する。ここで更新不要と判断すれば処理を終了し、また必要が生じた場合にバージョン情報取得処理を行うことになる。しかし、更新が必要と判断すれば (S 4 9)、次のファーム送信処理を実行する (S 5 0 ~ S 5 3)。この処理は、図 2 1 に示したファーム送信処理とほぼ同様であり、認証処理に用いるパスワードがパスワードリストに含まれるパスワード A である点が異なるのみである。

【0017】

以上の処理によって、必要な場合に被更新装置 9 2 のファームを更新することができる。そして、再度バージョン情報取得処理やファーム送信処理を行う場合は、再度パスワードリストを参照して使用するパスワードを決定する (S 5 4) が、ここでは、パスワード A が使用済みになっているので、次のパスワード B を選択することになる。

そして、ステップ S 5 5 ~ S 5 7 で、ステップ S 4 2 ~ S 4 4 の場合と同様に、バージョン情報取得処理を行うが、ここで認証に使用するパスワードはパスワード B となる。

以下、同様にして、パスワードをパスワード C, D, . . . と順次変更して処理を繰り返すことになる。

【0018】

このようにパスワードリストを用いるようにすれば、一度FTPを用いて転送したパスワードはファームウェア更新処理後には使用されることがなく、常に秘密の保たれたパスワードを使用して認証処理を行うことができるので、なりすまし等の不正アクセスを防止してセキュリティの向上を図ることができる。

しかしながら、このパスワードリストは多数のパスワードを含むため、データ量が多くなり、これを記憶する領域を用意するとメモリのコストアップにつながる。また、パスワードを装置に記憶させた状態にすることになるため、装置にアクセスした第3者にリストごとパスワードを盗まれる可能性も否定できない。また、初めにパスワードリストを郵便等によって送付し、管理者が手動で記憶させる必要があるので、労力がかかるという問題もあった。さらに、処理にエラーが生じて装置間で使用するパスワードのNo. が異なる事態が発生すると、認証処理が正常に行えないという問題もあった。また、パスワードリストに含まれるパスワードの数は有限であるので、全部使用してしまった後は、再度新たなリストを配布して記憶させるか、多少の危険を承知で使用済みのパスワードを再利用する必要があるという問題もあった。

【0019】

この発明は、これらの問題を解決し、ネットワークを介して通信可能な被更新装置のファームウェアをファームウェア更新装置によって更新する場合において、高い安全性を確保しながらコンパクトなソフトウェアによって更新処理を行うことができるようにすることを目的とする。

【0020】**【課題を解決するための手段】**

上記の目的を達成するため、この発明は、ネットワークを介して被更新装置と通信可能なファームウェア更新装置において、上記被更新装置のファームウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第1の通信経路で上記被更新装置に送信して記憶するよう要求する認証情報設定手段と、上記被更新装置に上記更新用認証情報を上記第1の通信経路よりも処理負荷の小さい第2の通信経路で送信し、その認証情報による認証処理を要求する認証要求手段と

、その認証処理が成功した場合に更新用ファームウェアを上記第2の通信経路で上記被更新装置に送信する送信手段とを設けたものである。

【0021】

このようなファームウェア更新装置において、上記更新用ファームウェアの送信後に、上記被更新装置に対して上記更新用認証情報の無効化要求を送信する認証情報無効化手段を設けるとよい。

さらに、上記被更新装置のファームウェアの更新を、外部からのファームウェア更新要求に応じて行い、その結果をその更新要求の要求元に返す手段を設けるとよい。

【0022】

さらに、上記被更新装置から起動した旨を示す起動通知を受け付ける手段と、上記更新用ファームウェアの送信後に上記被更新装置から上記起動通知を受け付けた場合にその被更新装置からファームウェアのバージョン情報を取得し、送信した更新用ファームウェアのバージョン情報と比較して更新の成否を確認する手段とを設けるとよい。

さらにまた、上記第1の通信経路をSSLによる通信を行う通信経路とし、上記第2の通信経路をFTPによる通信を行う通信経路とするとよい。

【0023】

また、この発明のファームウェア更新システムは、ネットワークを介して互いに通信可能なファームウェア更新装置と被更新装置とによって構成されるファームウェア更新システムにおいて、上記ファームウェア更新装置に、上記被更新装置のファームウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第1の通信経路で上記被更新装置に送信して記憶するよう要求する認証情報設定手段と、上記被更新装置に上記更新用認証情報を上記第1の通信経路よりも処理負荷の小さい第2の通信経路で送信し、その認証情報による認証処理を要求する認証要求手段と、その認証処理が成功した場合に更新用ファームウェアを上記第2の通信経路で上記被更新装置に送信する送信手段とを設け、上記被更新装置に、上記更新用認証情報を記憶するよう要求された場合にこれを記憶する記憶手段と、上記認証処理を要求された場合に、受信した更新用認証情報と上記記憶

手段に記憶している更新用認証情報とを用いて認証処理を行って結果を返す認証手段と、その認証処理が成功した場合に上記更新用ファームウェアを受信し、自機のファームウェアをその更新用ファームウェアに更新する更新手段とを設けたものである。

【0024】

このようなファームウェア更新システムにおいて、上記ファームウェア更新装置に、上記更新用ファームウェアの送信後に、上記被更新装置に対して上記更新用認証情報の無効化要求を送信する認証情報無効化手段を設け、上記被更新装置に、その無効化要求を受信した場合に上記記憶手段に記憶している更新用認証情報を無効化する手段を設けるとよい。

【0025】

さらに、上記被更新装置に、上記更新手段によるファームウェアの更新後に自機を再起動する手段と、起動時に上記ファームウェア更新装置にその旨を示す起動通知を送信する手段と、上記ファームウェア更新装置からの要求に応じてその装置にファームウェアのバージョン情報を送信する手段とを設け、上記ファームウェア更新装置に、上記更新用ファームウェアの送信後に上記被更新装置から上記起動通知を受け付けた場合にその被更新装置に対してファームウェアのバージョン情報の送信を要求してそのバージョン情報を取得し、送信した更新用ファームウェアのバージョン情報と比較して更新の成否を確認する手段を設けるとよい。

さらにまた、上記第1の通信経路をSSLによる通信を行う通信経路とし、上記第2の通信経路をFTPによる通信を行う通信経路とするとよい。

【0026】

また、この発明のファームウェア更新方法は、ファームウェア更新装置によって、ネットワークを介して通信可能な被更新装置のファームウェアを更新するファームウェア更新方法において、上記被更新装置のファームウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第1の通信経路で上記被更新装置に送信して記憶させ、上記被更新装置に上記更新用認証情報を上記第1の通信経路よりも処理負荷の小さい第2の通信経路で送信してその認証情報による認

証処理を行わせ、その認証処理が成功した場合に更新用ファームウェアを上記第2の通信経路で上記被更新装置に送信してファームウェアの更新を行わせるようにしたものである。

【0027】

このようなファームウェア更新方法において、上記更新用ファームウェアの送信後に、上記被更新装置に上記更新用認証情報を無効化させるようにするとよい。

さらに、上記被更新装置のファームウェアの更新を、外部からのファームウェア更新要求に応じて行い、その結果をその更新要求の要求元に返すようにするとよい。

【0028】

さらに、上記被更新装置から起動した旨を示す起動通知を受け付け、上記更新用ファームウェアの送信後に上記被更新装置から上記起動通知を受け付けた場合にその被更新装置からファームウェアのバージョン情報を取得し、送信した更新用ファームウェアのバージョン情報と比較して更新の成否を確認するようにするとよい。

さらにまた、上記第1の通信経路がSSLによる通信を行う通信経路であり、上記第2の通信経路がFTPによる通信を行う通信経路であるとよい。

【0029】

また、この発明のプログラムは、ネットワークを介して被更新装置と通信可能なファームウェア更新装置を制御するコンピュータを、上記被更新装置のファームウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第1の通信経路で上記被更新装置に送信して記憶するよう要求する認証情報設定手段と、上記被更新装置に上記更新用認証情報を上記第1の通信経路よりも処理負荷の小さい第2の通信経路で送信し、その認証情報による認証処理を要求する認証要求手段と、その認証処理が成功した場合に更新用ファームウェアを上記第2の通信経路で上記被更新装置に送信する送信手段として機能させるためのプログラムである。

【0030】

このようなプログラムにおいて、上記コンピュータを、上記更新用ファームウェアの送信後に、上記被更新装置に対して上記更新用認証情報の無効化要求を送信する認証情報無効化手段として機能させるためのプログラムをさらに含めるとよい。

また、上記コンピュータを、上記被更新装置のファームウェアの更新を外部からのファームウェア更新要求に応じて行い、その結果をその更新要求の要求元に返す手段として機能させるためのプログラムをさらに含めるとよい。

【0031】

また、上記コンピュータを、上記被更新装置から起動した旨を示す起動通知を受け付ける手段と、上記更新用ファームウェアの送信後に上記被更新装置から上記起動通知を受け付けた場合にその被更新装置からファームウェアのバージョン情報を取得し、送信した更新用ファームウェアのバージョン情報と比較して更新の成否を確認する手段として機能させるためのプログラムをさらに含めるとよい。

さらに、上記第1の通信経路をSSLによる通信を行う通信経路とし、上記第2の通信経路をFTPによる通信を行う通信経路とするとよい。

【0032】

【発明の実施の形態】

以下、この発明の好ましい実施の形態を図面を参照して説明する。

まず、この発明によるファームウェア更新装置及びファームウェア更新システムの構成例について説明する。図1は、そのファームウェア更新システムを含む遠隔管理システムの構成の一例を示す概念図であり、この図において仲介装置101がファームウェア更新装置、被管理装置10が被更新装置である。管理装置102をファームウェア更新装置としたり、この場合に仲介装置101を被更新装置としたりすることもできるが、ここでは、仲介装置101がファームウェア更新装置、被管理装置10が被更新装置である例について説明する。

【0033】

このファームウェア更新システムは、プリンタ、FAX装置、デジタル複写機、スキャナ装置、デジタル複合機等の画像処理装置や、ネットワーク家電、自動

販売機、医療機器、電源装置、空調システム、ガス・水道・電気等の計量システム等に通信機能を持たせた通信装置を被管理装置 10 とする遠隔管理システムの一部として構成される。そして、必要な場合に仲介装置 101 から被管理装置 10 にファームウェアを送信し、被管理装置 10 のファームウェアを更新させる機能を有する。

また、上記の遠隔管理システムは、被管理装置 10 と LAN（ローカルエリアネットワーク）によって接続された遠隔管理仲介装置である仲介装置 101、更に仲介装置 101 とインターネット 103（公衆回線等の他のネットワークでもよい）を介して接続されるサーバ装置として機能する管理装置 102 を備え、当該管理装置 102 が、仲介装置 101 を介して各被管理装置 10 を集中的に遠隔管理できるようにしたものである。当該仲介装置 101 及び被管理装置 10 は、その利用環境に応じて多様な階層構造を成す。

【0034】

例えば、図 1 に示す設置環境 A では、管理装置 102 と HTTP による直接的なコネクションを確立できる仲介装置 101a が、被管理装置 10a 及び 10b を従える単純な階層構造になっているが、同図に示す設置環境 B では、4 台の被管理装置 10 を設置する為、1 台の仲介装置 101 を設置しただけでは負荷が大きくなる。その為、管理装置 102 と HTTP による直接的なコネクションを確立できる仲介装置 101b が、被管理装置 10c 及び 10d だけでなく、他の仲介装置 101c を従え、この仲介装置 101c が被管理装置 10e 及び 10f を更に従えるという階層構造を形成している。この場合、被管理装置 10e 及び 10f を遠隔管理するために管理装置 102 から発せられた情報は、仲介装置 101b とその下位のノードである仲介装置 101c とを経由して、被管理装置 10e 又は 10f に到達することになる。

【0035】

また、設置環境 C のように、被管理装置 10 に仲介装置 101 の機能を併せ持たせた仲介機能付被管理装置 11a, 11b を、別途仲介装置を介さずにインターネット 103 によって管理装置 102 に接続するようにしてもよい。

図示はしていないが、仲介機能付被管理装置 11 の下位にさらに被管理装置 1

0 を接続することもできる。

なお、各設置環境には、セキュリティ面を考慮し、ファイアウォール 104 を設置する。

【0036】

このような遠隔管理システムにおいて、仲介装置 101 は、これに接続された被管理装置 10 の制御管理のためのアプリケーションプログラムを実装している。

管理装置 102 は、各仲介装置 101 の制御管理、更にはこの仲介装置 101 を介した被管理装置 10 の制御管理を行うためのアプリケーションプログラムを実装している。そして、被管理装置 10 も含め、この遠隔管理システムにおけるこれら各ノードは、RPC (Remote Procedure Call) により、相互の実装するアプリケーションプログラムのメソッドに対する処理の依頼である「要求」を送信し、この依頼された処理の結果である「応答」を取得することができるようになっている。

【0037】

すなわち、仲介装置 101 又はこれと接続された被管理装置 10 では、管理装置 102 への要求を生成してこれを管理装置 102 へ引き渡し、この要求に対する応答を取得できる一方で、管理装置 102 は、上記仲介装置 101 側への要求を生成してこれを仲介装置 101 側へ引き渡し、この要求に対する応答を取得できるようになっている。この要求には、仲介装置 101 に被管理装置 10 に対して各種要求を送信させ、被管理装置 10 からの応答を仲介装置 101 を介して取得することも含まれる。

なお、RPC を実現するために、SOAP (Simple Object Access Protocol : ソープ) , HTTP (HyperText Transfer Protocol) , FTP, COM (Component Object Model) , CORBA (Common Object Request Broker Architecture) 等の既知のプロトコル (通信規格) , 技術, 仕様などを利用することができる。

【0038】

この送受信のデータ送受モデルを図 2 の概念図に示す。

(A) は、被管理装置 10 で管理装置 102 に対する要求が発生したケースである。このケースでは、被管理装置 10 が被管理装置側要求 a を生成し、これを仲介装置 101 を経由して受け取った管理装置 102 がこの要求に対する応答 a を返すというモデルになる。同図に示す仲介装置 101 は複数であるケースも想定できる（上記図 1 に示す設置環境 B）。なお、(A) では、応答 a だけでなく応答遅延通知 a' を返信するケースが表記されている。これは、管理装置 102 が、仲介装置 101 を経由して被管理装置側要求を受け取って、当該要求に対する応答を即座に返せないと判断したときには、応答遅延通知を通知して一旦接続状態を切断し、次回の接続の際に上記要求に対する応答を改めて引き渡す構成としているためである。

【0039】

(B) は、管理装置 102 で被管理装置 10 に対する要求が発生したケースである。このケースでは、管理装置 102 が管理装置側要求 b を生成し、これを仲介装置 101 を経由して受け取った被管理装置 10 が、当該要求に対する応答 b を返すというモデルになっている。なお、(B) のケースでも、応答を即座に返せないときに応答遅延通知 b' を返すことは (A) のケースと同様である。

【0040】

次に、図 1 に示す管理装置 102 の物理的構成について説明すると、当該管理装置 102 は、不図示の CPU、ROM、RAM、不揮発性メモリ、ネットワークインタフェースカード（以下 NIC という）等を備えている。

また、図 1 に示す仲介装置 101 の物理的構成は、図 3 に示す通りである。

すなわち、CPU 52、SDRAM 53、フラッシュメモリ 54、RTC（リアルタイムクロック）55、Op-Port（操作部接続ポート）56、PHY（物理メディアインタフェース）57、モデム 58、HDD 制御部 59、拡張 I/F（インターフェース）60、RS232I/F 61、RS485I/F 62、HDD（ハードディスクドライブ）63等を備えている。そして、当該仲介装置 15 は PHY 57 を介して LAN と接続される。また、その LAN を介して被管理装置 10 と接続されるものである。RS232I/F 61 及び RS485I/F 62 を介しても被管理装置 10 と接続可能であるが、ここではこの I/F は使用し

ないものとする。

【0041】

なお、仲介機能付被管理装置 11 については、仲介装置 101 の機能を実現するためにこれらのユニットを単に被管理装置 10 に付加しても良いが、被管理装置 10 に備える CPU, ROM, RAM 等のハードウェア資源を利用し、CPU に適当なアプリケーションやプログラムモジュールを実行させることによって仲介装置 101 の機能を実現することもできる。

【0042】

図 4 は、仲介装置 101 のソフトウェア構成の一例を示すブロック図である。この図に示すように、仲介装置 101 のソフトウェアは、アプリケーション層 70, サービス層 80, プロトコル層 90 の 3 層からなっている。そして、これらのソフトウェアを構成するプログラムは HDD 63 や SDRAM 53、あるいはフラッシュメモリ 54 上に記憶され、必要に応じて読み出されて CPU 52 によって実行される。そして CPU 52 は、これらのプログラムを必要に応じて実行し、装置の制御を行うことにより、この発明による各機能（認証情報設定手段、認証要求手段、送信手段、その他の手段としての機能）を実現することができる。

【0043】

このソフトウェアにおいて、アプリケーション層 70 には、デバイスコントロールメソッド群 71 と NRS（ニュー・リモート・サービス）アプリケーションメソッド群 72 とを有する。

そして、デバイスコントロールメソッド群 71 は、管理対象情報設定、機器設定、ファームウェアアップデート、ポーリング設定変更、ログ出力、起動処理の各メソッドを備え、この発明の特徴に係るファームウェア更新処理を始め、被管理装置の情報管理や通信の設定等を行うためのプログラムである。

NRS アプリケーションメソッド群 72 は、ログ収集、ファームウェアダウンロード、機器コマンド実行、機器設定変更、サプライ通知、異常通知、デバイス起動／導入、デバイス生死確認の各メソッドを備え、被管理装置 10 からの種々の通知や要求に対応したり、管理装置 102 からの要求に従って被管理装置 10

に動作を行わせたりするためのプログラムである。

【0044】

次に、サービス層 80 には、セキュリティサービス 81，対接続機器通信サービス 82，対管理装置通信サービス 83，スケジューラサービス 84 とを備えている。

そして、セキュリティサービス 81 は、内部情報などの外部への不正流出を予防、妨害するなどのジョブを生成・実行するモジュールである。

対接続機器通信サービス 82 は、仲介装置 101 に接続されたネットワーク接続機器との間で情報の授受を実現するため、情報取得の対象となる機器の検索、対象機器との接続管理、ファイル送受信、パラメータ管理、A P L 管理などのジョブを生成・実行するモジュールである。

対管理装置通信サービス 83 は、管理装置 102 との間でコマンド受信、ファイル送受信、情報要求、情報送信（情報通知）などのジョブを生成・実行するモジュールである。

スケジューラサービス 84 は、所定の設定時間情報に基づき、リモートコントロールアプリを展開するモジュールである。

【0045】

次のプロトコル層 90 には、情報の送受信対象に応じたプロトコルを用いて情報の授受をおこなうジョブを生成・実行するための各メソッドを備える。即ち、L A N を介したネットワーク接続機器の通信環境に広く対応可能なように、S O A P (Simple Object Access Protocol) や、その下位プロトコルとして用いられる H T T P, H T T P S (Hypertext Transfer Protocol Security), F T P などを制御可能なメソッドを有している。

【0046】

以下、図 1 に示した遠隔管理システムのより具体的な例として、画像形成装置を被管理装置とした画像形成装置遠隔管理システムについて説明する。この遠隔管理システムは、画像形成装置を被更新装置とした、この発明によるファームウェア更新システムを含むものである。図 5 は、その画像形成装置遠隔管理システムの構成の一例を示す概念図であるが、被管理装置 10 を画像形成装置 100 に

、仲介機能付被管理装置 11 を仲介機能付画像形成装置 110 に変更した点が図 1 と相違するのみであるので、システムの全体構成についての説明は省略する。なお、ファームウェア更新システムは、この発明のファームウェア更新装置の実施形態である仲介装置 101 と被更新装置となる画像形成装置 100 のみで構成することができ、管理装置 102 やファイアウォール 104 等の他の構成要素は必須ではない。

【0047】

そして、画像形成装置 100 は、コピー、ファクシミリ、スキャナ等の機能及び外部装置と通信を行う機能を備えたデジタル複合機であり、それらの機能に係るサービスを提供するためのアプリケーションプログラムを実装しているものである。また、仲介機能付画像形成装置 110 は、画像形成装置 100 に仲介装置 101 の機能を併せ持たせたものである。

【0048】

このような画像形成装置 100 の物理的構成について図 6 を用いて説明する。

図 6 は、画像形成装置 100 内の物理的構成の一例を示すブロック図である。同図に示すように、画像形成装置 100 は、コントローラボード 200、HDD（ハードディスクドライブ）201、NV-RAM（不揮発性 RAM）202、PI（パーソナルインタフェース）ボード 203、PHY 204、操作パネル 205、プロッタ／スキャナエンジンボード 206、電源ユニット 207、フィニッシャ 208、ADF（自動原稿給送装置）209、給紙バンク 210、その他周辺機 211 を備えている。

【0049】

ここで、コントローラボード 200 は、制御手段に該当し、CPU、ROM、RAM等を備え、PCI-BUS（Peripheral Components Interconnect-Bus）212 を介して各機能を制御している。また、HDD 201 は、記憶手段に該当する。また、NV-RAM 202 は、記憶手段に該当し、不揮発性メモリであって、例えば、フラッシュメモリ等が該当する。

【0050】

また、PI ボード 203 と PHY 204 は、通信手段に該当し、外部との通信

を行うためのものであって、例えば、通信ボード等が該当する。P I ボード 2 0 3 は R S 4 8 5 規格に準拠したインタフェースを備え、ラインアダプタを介して公衆回線に接続している。P H Y 2 0 4 は、L A N を介して外部装置と通信を行うためのインタフェースであり、I E E E (Institute of Electrical and Electronic Engineers) 8 0 2 . 1 1 b 規格 (無線 L A N 対応), I E E E 1 3 9 4 規格, I E E E 8 0 2 . 3 規格 (イーサネット (登録商標) 対応) に準拠したインタフェースをそれぞれ設け、複数の通信手段としている。

また、操作パネル 2 0 5 は、操作部及び表示部に該当するユーザインタフェースである。

【0051】

ここで、同図中の E N G R D Y は、エンジン側の各種初期設定が完了して、コントローラボード 2 0 0 とコマンドの送受信の準備ができたことをコントローラボード 2 0 0 側に通知するための信号線である。また、P W R C T L は、エンジンへの電源供給をコントローラボード 2 0 0 側から制御するための信号線である。これら信号線の動作に関しては後述する。次に、画像形成装置 1 0 0 におけるソフトウェア構成を図 7 を用いて説明する。

【0052】

図 7 は、画像形成装置 1 0 0 のソフトウェア構成の一例を示すブロック図である。当該画像形成装置 1 0 0 のソフトウェア構成は、最上位のアプリケーションモジュール層、その下位のサービスモジュール層からなる。そして、これらのソフトウェアを構成するプログラムは H D D 2 0 1 やコントローラボード 2 0 0 上の R A M に記憶され、必要に応じて読み出されてコントローラボード 2 0 0 上の C P U によって実行される。そして C P U は、これらのプログラムを必要に応じて実行し、装置の制御を行うことにより、この発明による各機能 (記憶手段、認証手段、更新手段、その他の手段としての機能) を実現することができる。

【0053】

なお、C P U の機能のうち、管理装置 1 0 2 との通信に係わる機能の実現方法は、画像形成装置 1 0 0 と仲介機能付画像形成装置 1 1 0 とによって異なる。つまり、仲介機能付画像形成装置 1 1 0 の場合は、仲介装置の機能を備えているた

め、CPUが対応するプログラムを実行することにより、管理装置102との通信に係わる機能を実現することができる。画像形成装置100の場合には、CPUが対応するプログラムを実行すると共に、仲介装置101を利用することにより、管理装置102との通信に係わる機能を実現することができる。

【0054】

サービスモジュール層には、オペレーションコントロールサービス（OCS）300、エンジンコントロールサービス（ECS）301、メモリコントロールサービス（MCS）302、ネットワークコントロールサービス（NCS）303、ファクスコントロールサービス（FCS）304、ニューリモートサービス（NRS）305、システムコントロールサービス（SCS）306、システムリソースマネージャ（SRM）307、イメージメモリハンドラ（IMH）308、カスタマーサポートシステム（CSS）315、デリバリーコントロールサービス（DCS）316、ユーザコントロールサービス（UCS）317を実装している。更に、アプリケーションモジュール層には、コピーアプリ309、ファクスアプリ310、プリンタアプリ311、スキャナアプリ312、ネットファイルアプリ313、ウェブアプリ314を実装している。

【0055】

これらを更に詳述する。

OCS300は、操作パネル205を制御するモジュールである。

ECS301は、ハードウェアリソース等のエンジンを制御するモジュールである。

MCS302は、メモリ制御をするモジュールであり、例えば、画像メモリの取得及び開放、HDD201の利用等を行う。

NCS303は、ネットワークとアプリケーションモジュール層の各アプリケーションプログラムとの仲介処理を行わせるモジュールである。

FCS304は、ファクシミリ送受信、ファクシミリ読み取り、ファクシミリ受信印刷等を行うモジュールである。

NRS305は、ネットワークを介してデータを送受信する際のデータの変換等をするモジュールであり、またネットワークを介した遠隔管理に関する機能を

まとめたモジュールである。

【 0 0 5 6 】

SCS 3 0 6 は、コマンドの内容に応じたアプリケーションモジュール層の各アプリケーションプログラムの起動管理及び終了管理を行うモジュールである。

SRM 3 0 7 は、システムの制御及びリソースの管理を行うモジュールである。

IMH 3 0 8 は、一時的に画像データを入れておくメモリを管理するモジュールである。

CSS 3 1 5 は、公衆回線を介してデータを送受信する際のデータの変換等をするモジュールであり、また公衆回線を介した遠隔管理に関する機能をまとめたモジュールである。

DCS 3 1 6 は、HDD 2 0 1 やコントローラボード 2 0 0 上のメモリに記憶している（する）画像ファイル等をSMTP（Simple Mail Transfer Protocol）やFTP（File Transfer Protocol）を用いて送受信するモジュールである。

UCS 3 1 7 は、ユーザが登録した宛先情報や宛名情報等のユーザ情報を管理するモジュールである。

【 0 0 5 7 】

コピーアプリ 3 0 9 は、コピーサービスを実現するためのアプリケーションプログラムである。

ファクスアプリ 3 1 0 は、ファクスサービスを実現するためのアプリケーションプログラムである。

プリンタアプリ 3 1 1 は、プリンタサービスを実現するためのアプリケーションプログラムである。

スキャナアプリ 3 1 2 は、スキャナサービスを実現するためのアプリケーションプログラムである。

ネットファイルアプリ 3 1 3 は、ネットファイルサービスを実現するためのアプリケーションプログラムである。

ウェブアプリ 3 1 4 は、ウェブサービスを実現するためのアプリケーションプログラムである。

【0058】

ここで、上述したENGRDY信号とPWRC TL信号との動作を図8を用いて説明する。

図8の(A)は機器の立ち上がり時のENGRDY信号とPWRC TL信号の動作の一例を示している。AC-POWERのAC電源をONにすると電源供給が開始され、これと同時にENGRDY信号はHighになる。この状態ではエンジン側との通信はできない。なぜなら、エンジン側の初期設定が完了していないからである。そして、一定期間経過後にエンジン側の初期設定が完了し、ENGRDY信号がLowになった段階でエンジン側との通信が可能となる。

【0059】

次に、同図(B)は省エネモードに移行した時のENGRDY信号とPWRC TL信号の動作の一例を示している。省エネモードに移行するため、コントローラボード200によりPWRC TL信号をOFFにする。これと同時に電源供給もおちる。これに伴って、ENGRDY信号は、Highとなり省エネモードに移行する。次に、省エネモードから復帰する場合を同図(C)に示す。

【0060】

同図(C)は、省エネモードから復帰する時のENGRDY信号とPWRC TL信号の動作の一例を示している。上記(B)の省エネモードから復帰する際には、コントローラボード200によりPWRC TL信号をONにする。これと同時に電源供給もされる。しかし、上記の(A)で示したように、エンジン側の初期設定が完了するまで、ENGRDY信号はHighの状態であり、初期設定が完了するとエンジン側との通信が可能となり、Lowとなる。

【0061】

次に、上述した画像形成装置100のソフトウェアの構成に含まれるNRSモジュールの内部構成を図9を用いて更に説明する。

図9は、NRSモジュールの構成の一例を示す機能ブロック図である。同図に示すように、NRS305は、SCS306とNCS303との間で処理をおこなっている。ウェブサーバ機能部500は、外部から受信した要求に関する応答処理を行う。ここでの要求は、例えば、構造化言語であるXML (Extensible M

arkup Language) 形式で記載された、SOAP (Simple Object Access Protocol) による SOAP メッセージであることが考えられる。ウェブクライアント機能部 501 は、外部への要求を発行する処理を行う。libsoap502 は、SOAP を処理するライブラリであり、libxml503 は、XML 形式で記載されたデータを処理するライブラリである。また、libgwww504 は、HTTP を処理するライブラリであり、libgw__ncs505 は、NCS 303 との間の処理をするライブラリである。

【0062】

上述した構成を踏まえて、図 5 の画像形成装置遠隔管理システム内で行われるデータ送受信の際の通信シーケンスの一例について図 10 を用いて説明する。なお、以下に示す SCS 306 および NRS 305 による処理は、実際には CPU がそれらのプログラムに従って動作することによって実行するが、説明の都合上、それらのプログラムが処理を実行するものとする。以後も、プログラムが何らかの処理を行うものとして説明を行う場合には、同様とする。

【0063】

図 10 は、管理装置、仲介装置、及び画像形成装置間で行われるデータ送受信の際の通信シーケンスの一例を示す図である。

この例においては、まず、仲介装置 101 は、管理装置 102 に対してポーリング（送信要求があるかどうかの問い合わせ）を行う（S601）。つまり、自己の識別情報である識別子を付加したポーリング用の SOAP ドキュメントを生成し、HTTP メッセージとして管理装置 102 へ送信する。図 5 に示したように、仲介装置 101 と管理装置 102 との間にはファイアウォール 104 を設けているため、管理装置 102 から仲介装置 101 に向けて通信セッションを張る（通信を要求して通信経路を確立する）ことができないので、管理装置 102 から仲介装置 101（あるいは仲介装置 101 を介して画像形成装置 100）に要求を送信したい場合でも、このように仲介装置 101 からのポーリングを待つ必要があるのである。

【0064】

管理装置 102 は、仲介装置 101 から上記 HTTP メッセージを受信すると

、課金カウンタ取得要求を示すSOAPドキュメントを生成し、該当する仲介装置101（受信したSOAPメッセージの送信元）へ、ポーリングに対する応答のHTTPメッセージとして送信する（S602）。このとき、受信したHTTPメッセージ内のSOAPドキュメントに付加された識別子に基づいて該当する仲介装置101を認識する。このように、ファイアウォール104の内側からの通信（HTTPリクエスト）に対する応答（HTTPレスポンス）であれば、ファイアウォールの外側から内側に対してデータを送信することができる。

【0065】

仲介装置101は、管理装置102から上記HTTPメッセージを受信すると、そのHTTPメッセージに基づいて課金カウンタ取得要求を示すSOAPドキュメントを生成し、やはりHTTPメッセージとして自己に接続されている画像形成装置100へ送信し、画像形成装置100側ではウェブサービスアプリ318がこれを受け取る（S603）。

そして、ウェブサービスアプリ318が仲介装置101からHTTPメッセージとして受信したSOAPドキュメントに記述されている課金カウンタ取得要求をNRS305に渡し、NRS305がそれをSCS306へ通知する（S604）。

SCS306は、NRS305から課金カウンタ取得要求の通知を受けると、NV-RAM202に格納されている課金カウンタのデータを読み取る（S605）。そして、その読み取った課金カウンタのデータ（応答データ）をNRS305へ引き渡す（S606）。

【0066】

NRS305は、SCS306から課金カウンタのデータを受け取る（取得する）と、これをウェブサービスアプリ318に渡す。そして、ウェブサービスアプリ318がその内容を示す課金カウンタ用のSOAPドキュメントを生成し、HTTPメッセージとして仲介装置101へ送信する（S607）。

仲介装置101は、ウェブサービスアプリ318から課金カウンタ用のSOAPドキュメントを受信すると、そのSOAPドキュメントをHTTPメッセージとして管理装置102へ送信する（S608）。

このように、上記通信シーケンスにより、データの送受信が行われる。

【0067】

次に、上記図10と異なり、画像形成装置100から仲介装置101を経て管理装置102へデータを送信する場合の通信シーケンスの一例について図11を用いて説明する。

図11は、画像形成装置から管理装置102へデータを送信する場合の通信シーケンスの一例を示す図である。

この例においては、まず、OCS300は、ユーザコールキーが押下された旨をSCS306へ通知する(S701)。

SCS306は、OCS300からユーザコールキーが押下された旨の通知を受けると、ユーザコール要求をNRS305へ通知する(S702)。

【0068】

NRS305は、SCS306からユーザコール要求の通知を受けると、これをウェブサービスアプリ318に渡す。そして、ウェブサービスアプリ318がユーザコールを知らせるユーザコール情報であるユーザコール用のSOAPドキュメントを生成し、HTTPメッセージとして仲介装置101へ送信する(S703)。

仲介装置101は、ウェブサービスアプリ318からユーザコール用のSOAPドキュメントを受信すると、そのSOAPドキュメントに自己の識別情報である識別子を付加し、そのSOAPドキュメントをやはりHTTPメッセージとして管理装置102に対して送信し、ユーザコールを行う。つまり、自己の識別子を付加したユーザコール用のSOAPドキュメントを管理装置102へ通報する(S704)。この場合には、ファイアウォール104の内側から外側に向けての送信であるので、仲介装置101が自ら管理装置102に向けてセッションを張ってデータを送信することができる。

ここで、ステップS704の処理後のパターンを以下の(A)から(C)に分けて説明する。

【0069】

まず、(A)において、管理装置102は、ユーザ先の仲介装置101からユ

ーザコール用のSOAPドキュメントをHTTPメッセージとして受信し、その受信が正常に終了した場合には、その旨（ユーザコールが成功した旨）のコール結果を、正常に終了しなかった（異常に終了した）場合には、その旨（ユーザコールが失敗した旨）のコール結果を示すSOAPドキュメント生成し、HTTPメッセージによる応答として通報元の仲介装置101へ送信する（S705）。

仲介装置101は、管理装置102からコール結果を示すSOAPドキュメントを受信すると、そのSOAPドキュメントを、やはりHTTPメッセージとしてユーザコールキーが押下された画像形成装置100へ送信し、画像形成装置100側ではウェブサービスアプリ318がこれを受け取る（S706）。

【0070】

ウェブサービスアプリ318は、仲介装置101からコール結果を示すSOAPドキュメントを受信すると、そのSOAPドキュメントが示すコール結果をNRS305に渡す。そしてNRS305がそのコール結果を解釈（判定）し、SCS306へ通知する（S707）。

SCS306は、コール結果を受け取ると、それをOCS300へ引き渡す。

OCS300は、SCS306からコール結果を受け取ると、その内容つまりユーザコールが成功したか失敗したかを示すメッセージを操作パネル205上の文字表示器に表示する（S708）。

【0071】

次に（B）において、仲介装置101は、規定時間（予め設定された所定時間）が経っても管理装置102から応答がないと判断した場合には、ユーザコールが失敗した旨のコール結果を示すSOAPドキュメントを生成し、HTTPメッセージとしてウェブサービスアプリ318へ送信する（S709）。

ウェブサービスアプリ318は、失敗した旨のコール結果を示すSOAPドキュメントを受信すると、そのSOAPドキュメントに記述されている失敗した旨のコール結果をNRS305に渡す。そしてNRS305がそのコール結果を解釈し、SCS306へ通知する（S710）。

SCS306は、NRS305からコール結果を受け取ると、それをOCS300へ引き渡す。

OCS300は、SCS306からコール結果を受け取ると、その内容つまりユーザコールが失敗した旨を示すメッセージを操作パネル205上の文字表示器に表示する(S711)。

【0072】

次に(C)において、NRS305は、規定時間が経っても仲介装置101から応答がないと判断した場合には、ユーザコールが失敗した旨のコール結果をSCS306へ通知する(S712)。

SCS306は、NRS305からコール結果を受け取ると、それをOCS300へ引き渡す。

OCS300は、SCS306からコール結果を受け取ると、その内容つまりユーザコールが失敗した旨を示すメッセージを操作パネル205上の文字表示器に表示する(S713)。

【0073】

なお、ここでは管理装置102からファイアウォール104を越えて仲介装置101(あるいは仲介装置101を介して画像形成装置100)にデータを送信するために、仲介装置101からのHTTPリクエストに対するレスポンスという形で送信を行う例について説明したが、ファイアウォール104を越える手段はこれに限られるものではなく、例えば、SMTP(Simple Mail Transfer Protocol)を利用して、送信したいデータを記載あるいは添付したメールを管理装置102から仲介装置101に送信することも考えられる。ただし、信頼性の面ではHTTPが優れている。

【0074】

このような基本的な機能を有する図5に示した画像形成装置遠隔管理システムにおいて、仲介装置101と画像形成装置100との間の通信を、必要に応じてSSLを用いた相互認証を行ってから行うことができる。そこで次に、この相互認証を行う場合の通信手順について、認証処理の部分に焦点を当てて説明する。

図12は、仲介装置101と画像形成装置100とがSSLによる相互認証を行う際に各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

【0075】

図12に示すように、SSLによる相互認証を行う際には、まず仲介装置101側にルート鍵証明書、私有鍵A、公開鍵証明書Aを記憶しておく必要がある。私有鍵Aは、認証局（CA：certificate authority）が仲介装置101に対して発行した私有鍵である。そして、公開鍵証明書Aは、その私有鍵と対応する公開鍵にCAがデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、CAが付したデジタル署名の正当性を確認するための鍵であるルート鍵に、デジタル署名を付してデジタル証明書としたものである。なお、公開鍵は、対応する私有鍵を用いて暗号化された文書を復号化するための鍵本体と、その公開鍵の発行者（CA）、発行相手、有効期限等の情報を含む書誌情報とによって構成されるものとする。

【0076】

また、画像形成装置100側には、ルート鍵証明書、私有鍵B、公開鍵証明書Bを記憶しておく必要がある。私有鍵B及び公開鍵証明書Bは、CAが画像形成装置100に対して発行した私有鍵及び公開鍵証明書である。ここでは仲介装置101と画像形成装置100に対して同じCAが同じルート私有鍵を用いて証明書を発行しているものとし、この場合にはルート鍵証明書は仲介装置101と画像形成装置100で共通となる。

【0077】

フローチャートの説明に入る。なお、図12において、2本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信側はその情報を受信すると矢印の先端のステップの処理を行うものとする。また、各ステップの処理が正常に完了しなかった場合には、その時点で認証失敗の応答を返して処理を中断するものとする。相手から認証失敗の応答を受けた場合、処理がタイムアウトした場合等も同様である。また、それぞれの処理は、仲介装置101と画像形成装置100とがそれぞれ備えるCPUが所要の制御プログラムに従った処理を行うことにより実現されるものである。

【0078】

仲介装置101は、画像形成装置100に接続を要求する場合、図12の左側

に示すフローチャートの処理を開始する。そして、ステップS 2 1で画像形成装置100に対して接続要求を送信する。

一方画像形成装置100は、この接続要求を受信すると、図12の右側に示すフローチャートの処理を開始する。そして、ステップS 3 1で第1の乱数を生成し、これを私有鍵Bを用いて暗号化する。そして、ステップS 3 2でその暗号化した第1の乱数と公開鍵証明書Bとを仲介装置101に送信する。

【0079】

仲介装置101側では、これを受信すると、ステップS 2 2でルート鍵証明書を用いて公開鍵証明書Bの正当性を確認する。これには、公開鍵に含まれる書誌情報を参照して画像形成装置100が適当な通信相手であることを確認する処理を含む。

そして確認ができると、ステップS 2 3で、受信した公開鍵証明書Bに含まれる公開鍵Bを用いて第1の乱数を復号化する。ここで復号化が成功すれば、第1の乱数は確かに公開鍵証明書Bの発行対象である画像形成装置100から受信したものと確認できる。そして、画像形成装置100を正当な通信相手として認証する。

【0080】

その後、ステップS 2 4でこれとは別に第2の乱数及び第3の乱数を生成する。そして、ステップS 2 5で第2の乱数を私有鍵Aを用いて暗号化し、第3の乱数を公開鍵Bを用いて暗号化し、ステップS 2 6でこれらを公開鍵証明書Aと共に画像形成装置100に送信する。第3の乱数の暗号化は、画像形成装置100以外の装置に乱数を知られないようにするために行うものである。

【0081】

画像形成装置100側では、これを受信すると、ステップS 3 3でルート鍵証明書を用いて公開鍵証明書Aの正当性を確認する。これにも、ステップS 2 2の場合と同様、仲介装置101が適当な通信相手であることを確認する処理を含む。そして確認ができると、ステップS 3 4で、受信した公開鍵証明書Aに含まれる公開鍵Aを用いて第2の乱数を復号化する。ここで復号化が成功すれば、第2の乱数は確かに公開鍵証明書Aの発行対象である仲介装置101から受信したも

のだと確認できる。そして、画像形成装置 100 を正当な通信相手として認証する。

【0082】

その後、ステップ S35 で私有鍵 B を用いて第 3 の乱数を復号化する。ここまでの処理で、サーバ側とクライアント側に共通の第 1 乃至第 3 の乱数が共有されたことになる。そして、少なくとも第 3 の乱数は、生成した仲介装置 101 と、私有鍵 B を持つ画像形成装置 100 以外の装置が知ることはない。ここまでの処理が成功すると、ステップ S36 で仲介装置 101 に対して認証成功の応答を返す。

【0083】

仲介装置 101 側では、これを受信すると、ステップ S27 で第 1 乃至第 3 の乱数から共通鍵を生成し、以後の通信の暗号化に用いるものとして認証処理を終了する。画像形成装置 100 側でも、ステップ S37 で同様の処理を行って終了する。そして、以上の処理によって互いに通信を確立し、以後はステップ S27 又は S37 で生成した共通鍵を用い、共通鍵暗号方式でデータを暗号化して通信を行う。

なお、相互認証ではなく、画像形成装置 100 が仲介装置 101 を認証するのみでよいのであれば、第 1 及び第 3 の乱数の暗号化を省略することができる。この場合には、画像形成装置 100 側にはルート鍵証明書のみを記憶させておけばよい。

【0084】

通信の際にこのような SSL による相互認証を行えば、仲介装置 101 と画像形成装置 100 とが互いに相手を認証した上で安全に共通鍵を交換することができ、通信を確かな相手と安全に行うことができる。以下の説明において、これらのいずれかの装置が通信相手に対して SSL の接続要求を行う場合には、その要求に応じて図 12 に示したような相互認証処理を行い、認証が成功した場合に通信を確立するものとする。ただし、図 12 には仲介装置 101 から画像形成装置 100 に対して接続を要求する場合の処理を示しているので、画像形成装置 100 から仲介装置 101 に接続を要求する場合には、画像形成装置 100 が図 12

の仲介装置 101 に相当する処理を、仲介装置 101 が図 12 の画像形成装置 100 に相当する処理を行うことになる。

【0085】

次に、図 5 に示した画像形成装置遠隔管理システムにおけるこの発明の特徴に関連する動作である、画像形成装置 100 のファームウェア更新処理およびそのために必要な構成について説明する。この処理は、図 13 のシーケンス図に示す処理であり、この発明のファームウェア更新方法に係る処理であって、管理装置 102、仲介装置 101、画像形成装置 100 の各 CPU が、所要の制御プログラムを実行することによって行うものである。なお、仲介装置 101 がこの発明のファームウェア更新装置として機能し、画像形成装置 100 が被更新装置となる。そして、これらの装置によってこの発明のファームウェア更新システムが実現され、管理装置 102 はこのファームウェア更新システムにファームウェア更新要求を行う外部装置に該当する。

なお、図 13 に示す処理を行うに先立って、仲介装置 101 には予め更新用ファームウェアを記憶させておくものとする。この記憶は、管理装置 102 その他の装置から転送して行ってもよいし、記録媒体に記録したものを仲介装置 101 に読み込ませることによって行ってもよい。その他の適当な方法を採用することもできる。

【0086】

図 5 に示した画像形成装置遠隔管理システムにおいて、管理装置 102 は、所定時間毎あるいは管理装置 102 のオペレータから指示があった場合等、所定のイベントが発生した場合に、仲介装置 101 に対してファームウェア更新要求を送信する (S101)。図示は省略したが、この送信は、図 10 を用いて説明したように仲介装置 101 からのポーリングに対する応答として行うものである。

仲介装置 101 は、この要求を受けると、画像形成装置 100 のファーム更新に係る処理を開始するが、初めにワンタイムパスワード共有処理を行う (S102)。

【0087】

この処理において、まずステップ S102 で仲介装置 101 がファーム更新時

の認証処理に用いるための更新用認証情報としてワンタイムパスワードを乱数などにより生成し、これを記憶する。そして、画像形成装置 100 に対して SSL による接続要求を行う (S103)。この接続が確立すると、画像形成装置 100 にワンタイムパスワードを送信し、これを記憶するよう要求する (S104)。この要求は、SOAP による RPC としてなされる。

【0088】

画像形成装置 100 は、この要求に応じて受信したワンタイムパスワードを記憶手段に記憶し (S105)、以後 FTP 接続の際の認証処理において、仲介装置 101 の ID と対応するパスワードとして用いるものとする。認証は SSL の接続要求の際に完了しているので、ここではワンタイムパスワードを認証処理に用いることはない。そして、図示は省略したが、この記憶の終了後、画像形成装置 100 はその旨の応答を仲介装置 101 に返し、仲介装置 101 はこの応答を受け取ると SSL の接続を切断する (S106)。ステップ S103 乃至 S106 の通信は、HTTPS を用いて行われる。

【0089】

以上の処理がワンタイムパスワード共有処理であり、この処理において、仲介装置 101 の CPU 52 が認証情報設定手段として機能する。そしてこの処理によって、仲介装置 101 と画像形成装置 100 は、暗号化された通信経路を用いて安全にワンタイムパスワードを共有することができる。ここで用いた SSL による通信経路が、第 1 の通信経路である。なお、「通信経路」とは、物理的な伝送経路よりむしろ通信に使用するプロトコル (通信方式) によって定められるものである。従って、物理的な伝送経路が同一であっても通信プロトコルが異なれば「通信経路」は異なることになるし、逆にインターネットを介した通信のように物理的な伝送経路が状況に応じて変化する場合であっても、通信を行う装置と通信に使用するプロトコルが定まれば、「通信経路」は特定される。

【0090】

ワンタイムパスワード共有処理が終了すると、仲介装置 101 は次にバージョン情報取得処理を行う。

この処理は、従来の技術の項で図 21 に示した処理のステップ S11 乃至 S1

3 とほぼ同様なものであるが、仲介装置 101 がステップ S107 で F T P による接続を要求する際に画像形成装置 100 に送信するパスワードは、ステップ S104 で送信したものと同一ワнтаイムパスワードである。そして、画像形成装置 100 はステップ S105 で記憶したワнтаイムパスワードを用いて認証処理を行う。これらが一致すれば認証成功として接続を確立し（S107）、一致しなかった場合には接続は確立されず、エラーとなって処理は終了する。この処理において、仲介装置 101 の C P U 52 が認証要求手段として機能し、画像形成装置 100 の C P U が認証手段として機能する。

【0091】

接続が確立されると、画像形成装置 100 は仲介装置 101 からの要求に応じてファームのバージョン情報を送信する（S108）。仲介装置 101 はこのバージョン情報を取得し、その後、画像形成装置 100 との接続を切断する（S109）。以上がバージョン情報取得処理である。

次のステップ S110 の処理及びその後のファーム送信処理も、ワнтаイムパスワードを用いることを除き、図 21 に示した処理のステップ S14 乃至 S18 とほぼ同様なものである。

【0092】

すなわち、仲介装置 101 はステップ S108 で取得したファームのバージョン情報をもとに更新の要否を判断し、更新が必要と判断すれば（S110）、次のファーム送信処理を実行する。更新が不要と判断した場合には、管理装置 102 に対してファーム更新要求に対する応答としてその旨を通知するようにするとよい。

そして、ファーム送信処理では、仲介装置 101 はまずステップ S107 の場合と同様に画像形成装置 100 に I D とワнтаイムパスワードを送信し、画像形成装置 100 が認証処理を行って、成功すれば F T P による接続を確立する（S111）。そして、仲介装置 101 が更新用ファームウェアを画像形成装置 100 に送信する（S112）。この処理において、仲介装置 101 の C P U 52 が送信手段として機能する。

【0093】

画像形成装置 100 側では、これを受信すると、自機のファームウェアを受信した更新用ファームウェアに更新する (S113)。この処理においては、画像形成装置 100 の CPU が更新手段として機能する。そして、更新が完了すると自身をリセットし、再起動して新たなファームを有効にする (S114)。また、画像形成装置 100 のリセットにより、FTP 接続は切断される。以上がファーム送信処理である。

ここで用いた FTP による通信経路が、第 2 の通信経路である。FTP の場合には、通信内容の暗号化を行わないので、処理負荷は SSL を用いた第 1 の通信経路よりもはるかに小さい。

【0094】

画像形成装置 100 は、再起動が完了すると、起動した旨を示す起動通知として電源 ON 通知を仲介装置 101 に対して送信する (S115)。この電源 ON 通知は、SOAP ドキュメントとして記載し、HTTP を用いて送信することができる。

仲介装置 101 は、この電源 ON 通知を受信すると、ステップ S107～S109 の場合と同様にバージョン情報取得処理を行い、画像形成装置 100 との間で FTP による通信を確立し、画像形成装置 100 からファームのバージョン情報を取得する (S116～S118)。そして、このバージョン情報がステップ S112 で送信した更新用ファームウェアのものと一致していれば、ファームの更新が成功したと判断し (S119)、次のワンタイムパスワード消去処理を行う。一致していなければ、更新失敗と判断し、再度ファーム送信処理を行うか、あるいは管理装置 102 に対してファーム更新要求に対する応答として更新が失敗した旨を通知する。

なお、更新失敗と判断した場合であっても、画像形成装置 100 との間で SSL を用いた通信が可能であることが確認できた場合には、ワンタイムパスワード消去処理を行うようにしてもよい。

【0095】

次のワンタイムパスワード消去処理においては、仲介装置 101 はワンタイムパスワード共有処理の場合と同様に画像形成装置 100 に対して SSL による接

続要求を行う（S120）。そして、この接続が確立すると、画像形成装置100に消去用パスワードを送信し、これを記憶するよう要求する（S121）。この要求は、いわばワンタイムパスワードの無効化要求であり、この処理において、仲介装置101のCPU52が認証情報無効化手段として機能する。なお、消去用パスワードは、送信毎に作成するランダムなものであってもよいし、固定のパスワードでもよい。FTPによって送信しておらず、その後もFTPでは送信しないパスワードを用いればよい。また、この要求を行う際に、自身で記憶しているワンタイムパスワードも消去するようにしてもよい。

なお、ワンタイムパスワードの無効化要求は、記憶しているワンタイムパスワードを消去する要求であればよいのであるが、上述のようにパスワードの記憶（上書き）要求を用いるようにすれば、ワンタイムパスワードの共有の場合と処理を共通化し、プログラムのコンパクト化を図ると共に開発効率を向上させることができる。

【0096】

画像形成装置100は、この要求に応じてワンタイムパスワードを受信した消去用パスワードで上書きし（S122）、以後ステップS105で記憶したワンタイムパスワードはFTP接続の際の認証処理に用いないようにする。認証はSSLの接続要求の際に完了しているので、ここで消去用パスワードを認証処理に用いることはない。この記憶の終了後、仲介装置101はSSLの接続を切断する（S123）。

以上の処理がワンタイムパスワード消去処理であり、この処理によって、画像形成装置100に記憶させたワンタイムパスワードを無効化することができる。

このワンタイムパスワード消去処理が終了すると、仲介装置101は、管理装置102に対してファーム更新要求に対する応答として更新が成功した旨を通知する（S124）。

以上の処理を行うことにより、ネットワークを介して通信可能な被更新装置のファームウェアをファームウェア更新装置によって更新することができる。

【0097】

この処理をフローチャートで示したものが図14乃至図16である。これらの

図を用いて上述の処理についての説明を補足する。これらの図において、2本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信側はその情報を受信すると矢印の先端のステップの処理を行うものとする。

仲介装置101は、管理装置102からファーム更新要求を受け取ると、図14の左側に示すフローチャートの処理を開始する。そして、ステップS201でワンタイムパスワードを生成して記憶し、ステップS202で画像形成装置100に対してSSLによる接続要求を行う。

【0098】

画像形成装置100は、この要求を受け取ると図14の右側に示すフローチャートの処理を開始する。そして、ステップS301で仲介装置101側とSSLによる接続処理を行う。仲介装置101側のステップS202と画像形成装置100側のステップS301で行う処理が、図12に示した相互認証処理である。

認証が成功すると、画像形成装置100は図12のステップS36のように認証成功の応答を返す。すると、仲介装置101はステップS203で画像形成装置100にステップS201で生成したワンタイムパスワードを送信し、記憶するように要求する。画像形成装置100はこれを受け取ると、ステップS302で記憶し、記憶完了の応答を返す。仲介装置101は、この応答があるとステップS204で画像形成装置100に切断要求を送ってSSLによる接続を切断する。この要求を受けた仲介装置101もステップS303で接続を切断する。ここまでの処理がワンタイムパスワード共有処理である。

【0099】

次に、仲介装置101は、ステップS205で画像形成装置100に対してFTPの接続要求を行う。すると、画像形成装置100はステップS304で認証のためのIDとパスワードを要求するので、仲介装置101はこれに応じてステップS206でIDとステップS201で生成したワンタイムパスワードを送信する。

画像形成装置100はこのIDとパスワードを用いて認証処理を行い、これらが記憶しているものと一致すれば認証成功としてその旨の応答を返す。そして、

これを受けた仲介装置 101 は、ステップ S 207 で画像形成装置 100 に対してバージョン情報取得要求を送信してファームのバージョン情報を求める。画像形成装置 100 はこれに応じてステップ S 306 で仲介装置 101 にバージョン情報を送信し、仲介装置 101 はこれを取得するとステップ S 208 で F T P 接続を切断する。ここまでの処理がバージョン情報取得処理である。

なお、ステップ S 305 で認証が失敗した場合には、ステップ S 307 に進んでエラー処理を行うが、この処理としては、仲介装置 101 に認証失敗を通知して再度接続要求を待つ状態に移行することが考えられる。

図示は省略したが、ステップ S 301 等で S S L による相互認証が失敗した場合にも、同様な処理を行うようにするとよい。

【0100】

一方仲介装置 101 は、ステップ S 208 の次にステップ S 209 に進み、ステップ S 207 で取得したバージョン情報が最新バージョンのものか否かをもとに、画像形成装置 100 のファームを更新する必要があるか否か判断する。そして、更新する必要がある場合は、ステップ S 210 に進んでファーム送信処理を行う。

この場合、仲介装置 101 はステップ S 210 でステップ S 205 及び S 206 と同様な処理を、画像形成装置 100 はステップ S 308 でステップ S 304 及び S 305 と同様な処理を行って F T P 接続を確立する。ここで用いるパスワードも、ステップ S 206 の場合と同じワнтаイムパスワードである。

【0101】

接続が確立すると、仲介装置 101 はステップ S 211 で画像形成装置 100 に更新用ファームウェアを送信し、画像形成装置 100 はステップ S 309 でこれを受信すると、ステップ S 310 で自機のファームウェアをその更新用ファームウェアに更新する。このとき、他のジョブが実行中であつたり、予約されていたりした場合には、それが完了するまでは更新せずに待機するようにしてもよい。ファームウェアの更新が完了すると、画像形成装置 100 はステップ S 311 で自身をリセットし、再起動して新たなファームを有効にする。また、画像形成装置 100 のリセットにより、F T P 接続は切断される。以上がファーム送信処

理である。

【0102】

続いて、画像形成装置100の再起動が完了すると、画像形成装置100は起動したことを示す電源ON通知を仲介装置101に送信する。すると、仲介装置101はこれに応じてステップS212で画像形成装置100に対してFTPによる通信を要求し、以下ステップS214までで、ステップS205～S208と同様な処理を行って画像形成装置100からファームのバージョン情報を取得する。画像形成装置側でも、ステップS313及びS314で、ステップS304乃至S307の場合と同様な処理を行ってファームのバージョン情報を送信する。

【0103】

そして、仲介装置101はステップS215で、ステップS213で取得したバージョン情報と、ステップS211で送信した更新用ファームウェアのバージョン情報を比較し、一致していれば更新成功と判断して図16のステップS217に進む。一致していなければ、更新失敗と判断してステップS216に進み、エラー処理を行う。このエラー処理としては、再度S210からのファーム送信処理を行って画像形成装置100のファームウェアの更新を試みることに、あるいはファーム更新要求の送信元である管理装置102に対して、更新が失敗した旨の応答を返すことが考えられる。後者の場合には、処理を終了し、再度のファーム更新要求を待つことになる。

【0104】

ステップS215の判断がYESであり、図16のステップS217に進むと、ワンタイムパスワード無効化処理を開始し、仲介装置101はステップS202の場合と同様に画像形成装置100に対してSSLによる接続処理を行い、画像形成装置100側のステップS315の処理と併せて相互認証を行う。そして、画像形成装置100側から認証成功の応答が返されると、仲介装置101はステップS218で画像形成装置100に対して消去用パスワードを送信し、これを記憶するよう要求する。画像形成装置100はこれを受け取ると、ステップS316で記憶していたワンタイムパスワードに消去用パスワードを上書き記憶し

、記憶完了の応答を返す。仲介装置101は、この応答があるとステップS219で画像形成装置100に切断要求を送ってSSLによる接続を切断する。この要求を受けた仲介装置101もステップS317で接続を切断する。ここまでの処理がワンタイムパスワード無効化処理である。

なお、この処理において、記憶しているワンタイムパスワードを消去できるのであれば必ずしも上書きをしなくてもよいことは、上述した通りである。

【0105】

この処理は、消去用パスワードを必ずしも毎回生成する必要がない点を除けば、ワンタイムパスワード共有処理と同様なものである。しかし、このような処理によって、画像形成装置100がFTPの認証処理に用いるパスワードを別のパスワードに変更すれば、漏洩の危険性がある元のワンタイムパスワードを無効化でき、第3者によるなりすましを防止できる。また、消去用パスワードはFTPでは転送しないようにすれば、これが漏洩することもない。

【0106】

ワンタイムパスワード無効化処理の後、仲介装置101はステップS220で管理装置102にファームウェア更新についての結果を通知し、処理を終了する。

なお、ステップS209でファームの更新が不要と判断した場合には、そのまま図16のステップS217に進んでワンタイムパスワード無効化処理を行い、ステップS220で管理装置102に結果を通知して終了する。画像形成装置100側の処理は、基本的に仲介装置101からのトリガに応じて行うので、ステップS210やステップS212での要求がなければ、画像形成装置100は図15に示した部分の処理は行わない。

【0107】

以上説明したような処理を行うことにより、ネットワークを介して通信可能な被更新装置のファームウェアをファームウェア更新装置によって更新する場合において、高い安全性を確保しながらコンパクトなプログラムによって更新処理を行うことができる。

すなわち、まずファームの更新に必須のバージョン情報取得処理及びファーム

送信処理は処理負荷の小さい F T P によって行うようにしているので、プログラムをコンパクトにまとめることができる。ファーム自体は特に秘密にする必要のあるデータではないので、F T P などの暗号化を行わない通信で問題なく、むしろ処理負荷を低減してプログラムをコンパクトにする要求が強いのである。

【 0 1 0 8 】

一方で、不正なファームを受信しないようにするためには、通信相手の認証が重要となるが、F T P での認証処理に使用するパスワードは、使用する直前に生成して、通信内容を暗号化する S S L を用いて仲介装置 1 0 1 と画像形成装置 1 0 0 とが共有するようにしている。従って、このパスワードが第 3 者に漏洩することはなく、第 3 者が仲介装置 1 0 1 になりすまして別の装置から画像形成装置 1 0 0 に不正なファームを送信し、これに更新させてしまうといった事態を防止できる。

また、F T P での認証処理に使用したパスワードを、ファームの更新成功を確認した後ただちに無効化してしまうようにすれば、第 3 者が F T P による通信をモニタリングしてワнтаイムパスワードを不正に取得したとしても、後日そのパスワードを用いて接続される可能性はなく、不正なアクセスを防止することができる。

【 0 1 0 9 】

また、ファームウェアの更新に失敗した場合に備えて、被更新装置にはファームウェア自体の他にファームウェア更新処理用の更新プログラムを備えることは従来の技術の項で述べたが、上述の処理において、ファームの更新に失敗した場合にはワнтаイムパスワードを無効化しないようにしておけば、更新に失敗したとしても、S S L を使用しないバージョン情報取得処理からやり直すことができるので、画像形成装置 1 0 0 における更新プログラムとして用意するのは、バージョン情報取得処理及びファーム送信処理のためのプログラムのみでよい。従って、パスワードの受け渡しに S S L を使用して安全性を向上させながら、この処理に必要な部分を更新プログラムに含める必要がなく、更新プログラムをコンパクトにすることができる。

【 0 1 1 0 】

また、ファーム更新後に画像形成装置 100 が再起動した時点でファームのバージョン情報を確認するようにすれば、仲介装置 101 側で更新の成否を容易に知ることができる。そして、失敗していた場合に速やかに再更新等の対応を行うことができる。画像形成装置 100 が起動時にその旨を仲介装置 101 に通知するようにすれば、容易にこの確認のタイミングを計ることができる。

さらにまた、仲介装置 101 が外部からの要求に応じて画像形成装置 100 にファームウェアを更新させ、その結果を応答として返すようにすれば、各画像形成装置 100 におけるファームの更新状況を管理装置 102 等によって管理することができる。

【0111】

なお、ワンタイムパスワードの無効化について、上述した処理では、これを消去用パスワードの上書きによって行うようにすることにより、ワンタイムパスワードの共有の場合と処理を共通化し、プログラムのコンパクト化を図っている。

しかし、消去用パスワードの上書き要求に代えて、単に記憶しているワンタイムパスワードを認証処理に用いないようにする要求を行い、画像形成装置がこれに応じてワンタイムパスワードによる認証処理を行わない旨の設定を行うようにしてもよい。このようにする場合、要求自体を秘匿する必要はないので、必ずしも SSL による通信を行う必要はない。画像形成装置 100 から消去用パスワードが盗まれる危険性を考慮するのであれば、このような設定が有効になる。

【0112】

〔変形例〕

以下、上述した実施形態に適用できる種々の変形例について説明する。

以上説明した実施形態においては、仲介装置 101 が管理装置 102 からファーム更新要求を受けた場合にファームの更新処理を開始し、この際に仲介装置 101 がワンタイムパスワードを生成する例について説明した。しかし、この発明に係るファームの更新処理は、これに限られるものではない。

【0113】

まず、第 1 の変形例として、ワンタイムパスワードの生成を画像形成装置 100 側で行うようにしてもよい。この場合、図 13 のステップ S101 乃至 S10

6 の処理に代えて、図 17 に示す処理を行う。

すなわち、仲介装置 101 がステップ S101 でファーム更新要求を受けると、画像形成装置 100 のファーム更新に係る処理を開始するが、初めに画像形成装置 100 に対してワンタイムパスワード生成要求を送信する (S401)。この要求自体は特に秘匿する必要はないので、SOAP ドキュメントとして HTTP によって送信することができる。

【0114】

そして、画像形成装置 100 はこれに応じてワンタイムパスワードを生成し、これを記憶する (S402)。そしてこのワンタイムパスワードを、以後 FTP 接続の際の認証処理において、ワンタイムパスワード生成要求の送信元である仲介装置 101 の ID と対応するパスワードとして用いるものとする。

その後、画像形成装置 100 は仲介装置 101 に対して SSL による接続要求を行う (S403)。この接続が確立すると、仲介装置 101 にワンタイムパスワードを送信し、これを記憶するよう要求する (S404)。この要求は、SOAP による RPC としてなされる。

【0115】

画像形成装置 100 は、この要求に応じて受信したワンタイムパスワードを記憶手段に記憶し (S405)、以後 FTP 接続の際の認証処理において、このワンタイムパスワードを送信するものとする。そして、図示は省略したが、この記憶の終了後、仲介装置 101 はその旨の応答を画像形成装置 100 に返し、画像形成装置 100 はこの応答を受け取ると SSL の接続を切断する (S406)。ステップ S403 乃至 S406 の通信は、HTTPS を用いて行われる。

そして、ステップ S402 乃至 S406 の処理において、画像形成装置 100 の CPU が認証情報設定手段として機能する。

このような処理によっても、図 13 に示した処理の場合と同様に、仲介装置 101 と画像形成装置 100 が暗号化された通信経路を用いて安全にワンタイムパスワードを共有することができる。従って、図 13 に示した処理を行う場合と同様な効果を得ることができる。

【0116】

また、第2の変形例として、画像形成装置100が、操作パネル205等から直接ファームウェアの更新指示を受け付けることができるようにしてもよい。この場合、図13のステップS101乃至S106の処理に代えて、図18に示す処理を行う。

すなわち、画像形成装置100がファームウェアの更新指示を受け付けた場合（S411）、画像形成装置100のファーム更新に係る処理を開始し、仲介装置101に対してワンタイムパスワード生成要求を送信するようにする（S412）。そして仲介装置101は、この要求を受け取ると、図13に示した処理で管理装置102からファーム更新要求を受け取った場合と同様に、ワンタイムパスワード共有処理を行う。すなわち、ステップS413～S417では、図13のステップS102～S106と同様な処理を行う。

【0117】

このようにすれば、画像形成装置100が直接ファームウェアの更新指示を受け付けた場合でも、管理装置102からファーム更新要求があった場合と同様に画像形成装置100のファームウェアを更新することができる。

なお、この変形例では管理装置102からのファーム更新要求はないが、管理装置102が特定できるのであれば、ステップS124の更新結果通知は行うようにするとよい。このようにすれば、管理装置102は自身以外からの指示によるファームの更新状況も把握でき、適切な管理を行うことができる。

また、仲介装置101がOp-Port56に接続する操作部から直接ファームウェアの更新指示を受け付け、これに応じて画像形成装置100のファーム更新に係る処理（ワンタイムパスワード共有処理以降の処理）を開始できるようにしてもよい。

【0118】

第3の変形例としては、第1の変形例と第2の変形例を組み合わせることが考えられる。すなわち、画像形成装置100が、直接ファームウェアの更新指示を受け付け、さらにワンタイムパスワードの生成を画像形成装置100側で行うようにするのである。

この場合、図13のステップS101乃至S106の処理に代えて、図19に

示す処理を行う。

【0119】

この処理は、ステップS411の処理は図18の場合と同様であり、ステップS402～S406の処理は図17の場合と同様であるので、詳細な説明は省略するが、この場合には、仲介装置101は、ステップS404でワンタイムパスワードの記憶要求があった時点で画像形成装置100のファーム更新に係る処理が開始されたものと認識し、以後の処理を行うものとする。

この変形例の効果は、第1の変形例の効果と第2の変形例の効果を含めたものになる。

【0120】

第4の変形例としては、ワンタイムパスワード消去処理において、消去用パスワードの記憶要求を画像形成装置100側から行うようにすることができる。この場合、図13のステップS120乃至S123の処理に代えて、図20に示す処理を行う。

すなわち、画像形成装置100がまず図18のステップS412の場合と同様に仲介装置101に対してSSLによる接続要求を行う（S421）。そして、この接続が確立すると、仲介装置101に消去用パスワードを送信し、これを記憶するよう要求する（S422）。この要求は、いわばワンタイムパスワードの無効化要求であり、この処理において、画像形成装置100のCPUが認証情報無効化手段として機能する。

【0121】

仲介装置101は、この要求に応じてワンタイムパスワードを受信した消去用パスワードで上書きし（S423）、それまで記憶していたワンタイムパスワードは以後FTP接続の際に送信しないようにする。一方、画像形成装置100自身も、記憶しているワンタイムパスワードを消去用パスワードで上書きし（S424）、それまで記憶していたワンタイムパスワードは以後FTP接続の際の認証処理に用いないようにする。これらの記憶の終了後、画像形成装置100はSSLの接続を切断する（S425）。

この変形例は、上述した実施形態及び各変形例に適用できるが、第1及び第3

の変形例のように、画像形成装置 100 側でワンタイムパスワードを生成する場合に適用すると、SSL によるパスワードの送信処理を画像形成装置 100 側に統一できてプログラムの簡略化に効果的である。

なお、この変形例を適用する場合、仲介装置 101 が、図 13 のステップ S 119 でファームの更新が成功したと判断した場合に画像形成装置 101 に対してその旨を通知するようにし、画像形成装置 101 がその通知を受け取った場合に図 20 に示す処理を開始するようにするとよい。

【0122】

また、以上の実施形態及び各変形例においては、被更新装置の例として通信機能を備えた画像形成装置について主に説明したが、この発明はこれに限られるものではなく、通信機能を備えたネットワーク家電、自動販売機、医療機器、電源装置、空調システム、ガス・水道・電気等の計量システム等や、ネットワークに接続可能なコンピュータ等も含め、通信機能を備えた各種電子装置に適用可能である。また、ファームウェア更新装置についても、図 1 及び図 3 等にした仲介装置に限られるものではなく、ファームウェア更新の専用装置であったり、あるいは管理装置 102 であってもよい。

【0123】

さらに、この発明のファームウェア更新システムは、必ずしも遠隔管理システムに含まれるものとは限らず、また、被更新装置、ファーム更新装置、管理装置の構成及びこれらの接続形式は、以上の実施形態に限られるものではない。これらの各装置の間の通信も、有線、無線を問わず、ネットワークを構築可能な各種通信回線（通信経路）を用いて行うことができる。

また、通信経路について、第 1 の通信経路として SSL による通信経路、第 2 の通信経路として FTP による通信経路を用いた例について説明したが、これに限られるものではなく、第 1 の通信経路が暗号化されたものであり、第 2 の通信経路が第 1 の通信経路よりも処理負荷の小さいものであれば、他のプロトコルを使用した通信経路（通信方式）であっても構わない。

【0124】

また、この発明によるプログラムは、ネットワークを介して被更新装置と通信

可能なファームウェア更新装置を制御するコンピュータに、この発明による各機能（認証情報設定手段、認証要求手段、送信手段、その他の手段としての機能）を実現させるためのプログラムであり、このようなプログラムをコンピュータに実行させることにより、上述したような効果を得ることができる。

【0125】

このようなプログラムは、はじめからコンピュータに備えるROMあるいはHDD等の記憶手段に格納しておいてもよいが、記録媒体であるCD-ROMあるいはフレキシブルディスク、SRAM、EEPROM、メモリカード等の不揮発性記録媒体（メモリ）に記録して提供することもできる。そのメモリに記録されたプログラムをコンピュータにインストールしてCPUに実行させるか、CPUにそのメモリからこのプログラムを読み出して実行させることにより、上述した各手順を実行させることができる。

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外部機器あるいはプログラムを記憶手段に記憶した外部機器からダウンロードして実行させることも可能である。

【0126】

【発明の効果】

以上説明してきたように、この発明のファームウェア更新装置、ファームウェア更新システム、ファームウェア更新方法によれば、高い安全性を確保しながらコンパクトなソフトウェアによってファームウェアの更新処理を行うことができる。

また、この発明のプログラムによれば、コンピュータにファームウェア更新装置を制御させてこのようなファームウェア更新装置の特徴を実現し、同様な効果を得ることができる。

【図面の簡単な説明】

【図1】

この発明によるファームウェア更新システムを含む遠隔管理システムの構成例を示す概念図である。

【図2】

その遠隔管理システムにおけるデータ送受モデルを示す概念図である。

【図 3】

その遠隔管理システムを構成する仲介装置のハードウェア構成例を示すブロック図である。

【図 4】

その仲介装置のソフトウェア構成例を示すブロック図である。

【図 5】

画像形成装置を被更新装置としたこの発明によるファームウェア更新システムを含む、画像形成装置遠隔管理システムの構成例を示す概念図である。

【図 6】

その画像形成装置遠隔管理システムを構成する画像形成装置のハードウェア構成例を示すブロック図である。

【図 7】

その画像形成装置のソフトウェア構成例を示すブロック図である。

【図 8】

その画像形成装置における ENGRDY 信号と PWRC TL 信号について説明するための図である。

【図 9】

その画像形成装置におけるウェブサービスアプリの構成例を示す機能ブロック図である。

【図 10】

図 3 に示した画像形成装置遠隔管理システム内で行われるデータ送受信の際の通信シーケンスの一例を示す図である。

【図 11】

図 3 に示した画像形成装置から管理装置 102 へデータを送信する場合の通信シーケンスの一例を示す図である。

【図 12】

図 3 に示した仲介装置と画像形成装置との間で SSL を用いた相互認証を行う際の処理例を示す図である。

【図 1 3】

図 3 に示した仲介装置によって画像形成装置のファームウェアを更新する際の処理例を示すシーケンス図である。

【図 1 4】

図 3 に示した仲介装置によって画像形成装置のファームウェアを更新する際の処理例の一部を示すフローチャートである。

【図 1 5】

図 1 4 の続きの処理を示すフローチャートである。

【図 1 6】

図 1 5 の続きの処理を示すフローチャートである。

【図 1 7】

図 1 3 に示した処理の第 1 の変形例において図 1 3 の処理と入れ替える部分の処理例を示すシーケンス図である。

【図 1 8】

同じく第 2 の変形例において図 1 3 の処理と入れ替える部分の処理例を示すシーケンス図である。

【図 1 9】

同じく第 3 の変形例において図 1 3 の処理と入れ替える部分の処理例を示すシーケンス図である。

【図 2 0】

同じく第 4 の変形例において図 1 3 の処理と入れ替える部分の処理例を示すシーケンス図である。

【図 2 1】

従来のファームウェア更新システムにおけるファームウェア更新処理の例を示すシーケンス図である。

【図 2 2】

図 2 1 に示した処理の危険性について説明するための図である。

【図 2 3】

従来の別のファームウェア更新システムにおけるファームウェア更新処理に用

いるパスワードリストの例を示す図である。

【図 24】

その別のファームウェア更新システムにおけるファームウェア更新処理の例を示すシーケンス図である。

【符号の説明】

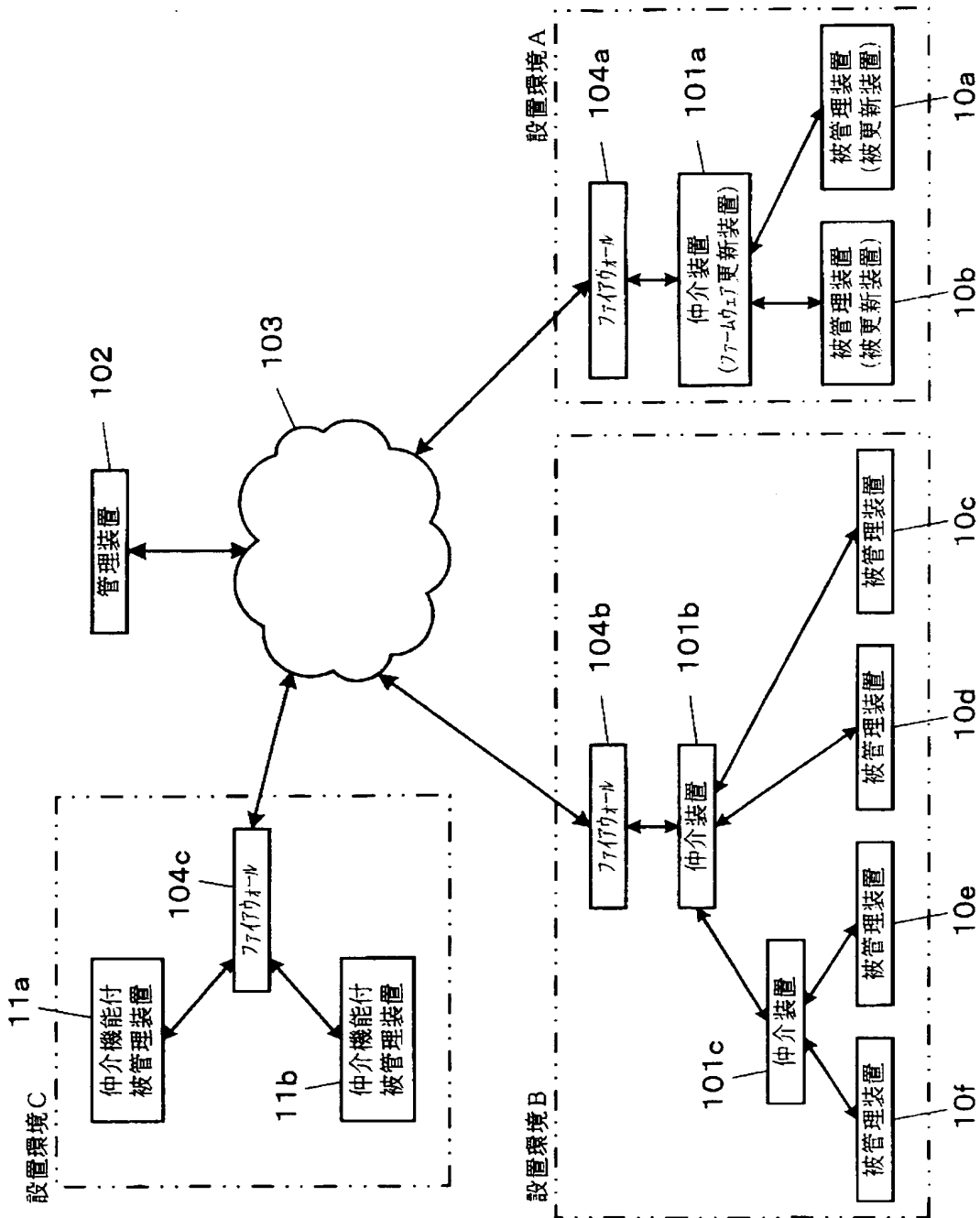
10: 被管理装置	11: 仲介機能付被管理装置
52: CPU	53: SDRAM
54: フラッシュメモリ	55: RTC
56: Op-Port	57: PHY
58: モデム	59: HDD制御部
63: HDD	70: アプリケーション層
80: サービス層	90: プロトコル層
100: 画像形成装置	101: 仲介装置
102: 管理装置	103: インタネット
104: ファイアウォール	105: 端末装置
110: 仲介機能付画像形成装置	
200: コントローラボード	201: HDD
202: NV-RAM	203: PIボード
204: PHY	205: 操作パネル
206: プロッタ/スキャナエンジンボード	
207: 電源ユニット	212: PCI-BUS
300: OCS	301: ECS
302: MCS	303: NCS
304: FCS	305: NRS
306: SCS	307: SRM
308: IMH	309: コピーアプリ
310: ファクスアプリ	311: プリンタアプリ
312: スキャナアプリ	
313: ネットファイルアプリ	314: ウェブアプリ

3 1 5 : C S S

3 1 6 : D C S

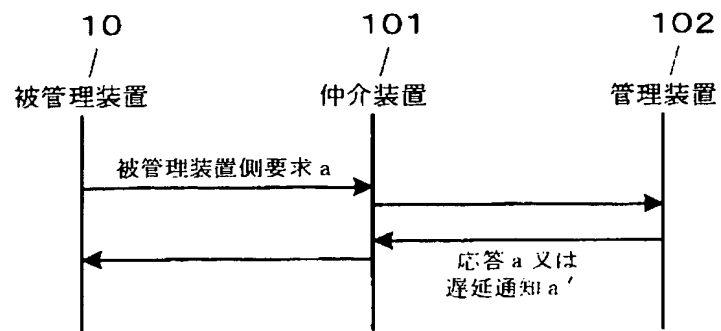
【書類名】 図面

【図 1】

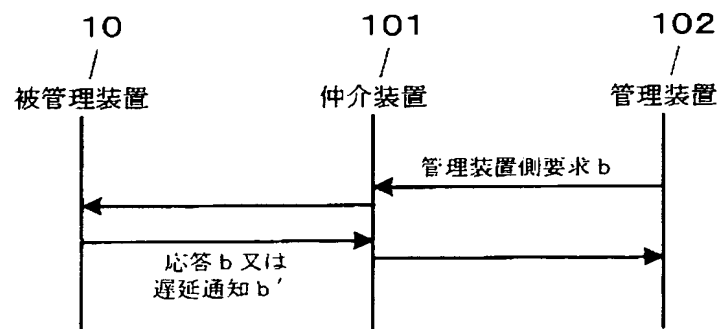


【図 2】

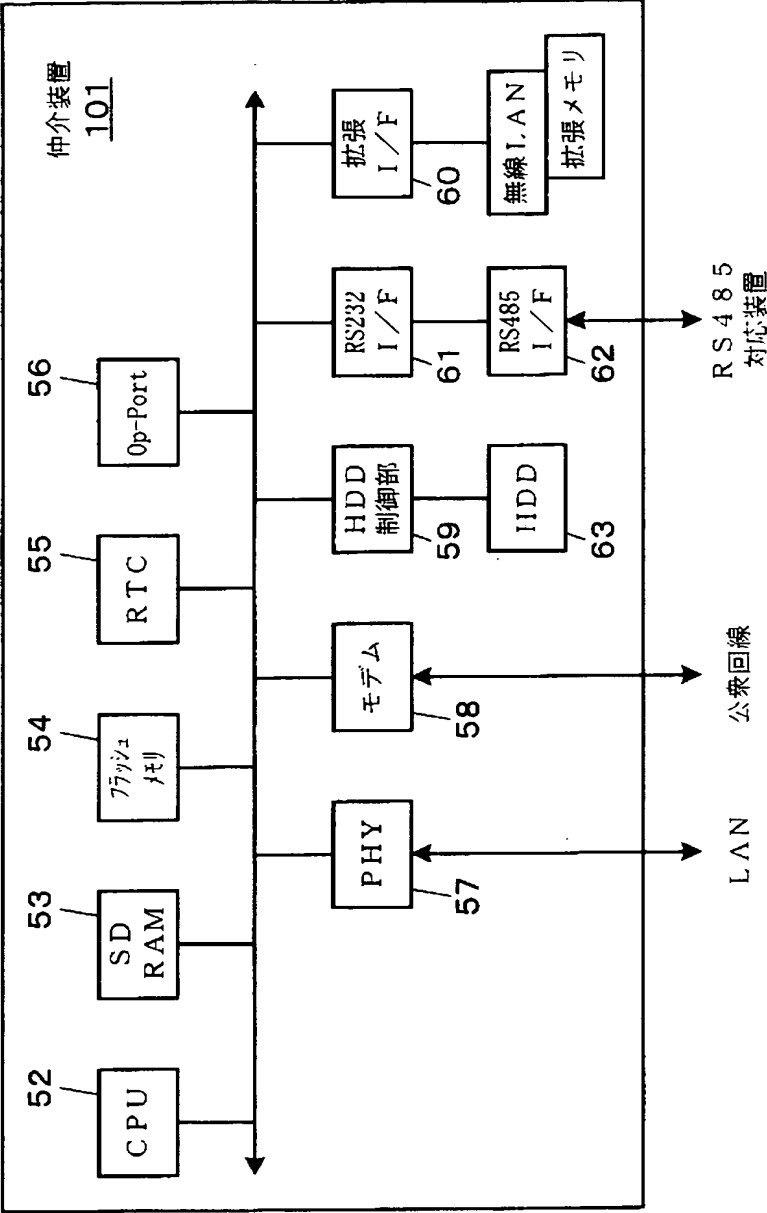
(A)



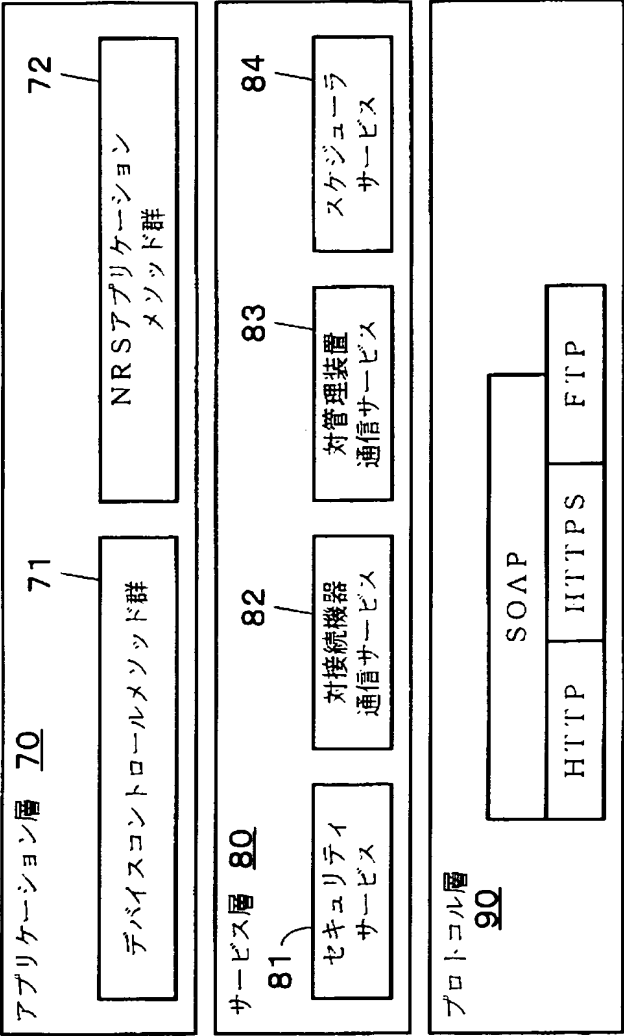
(B)



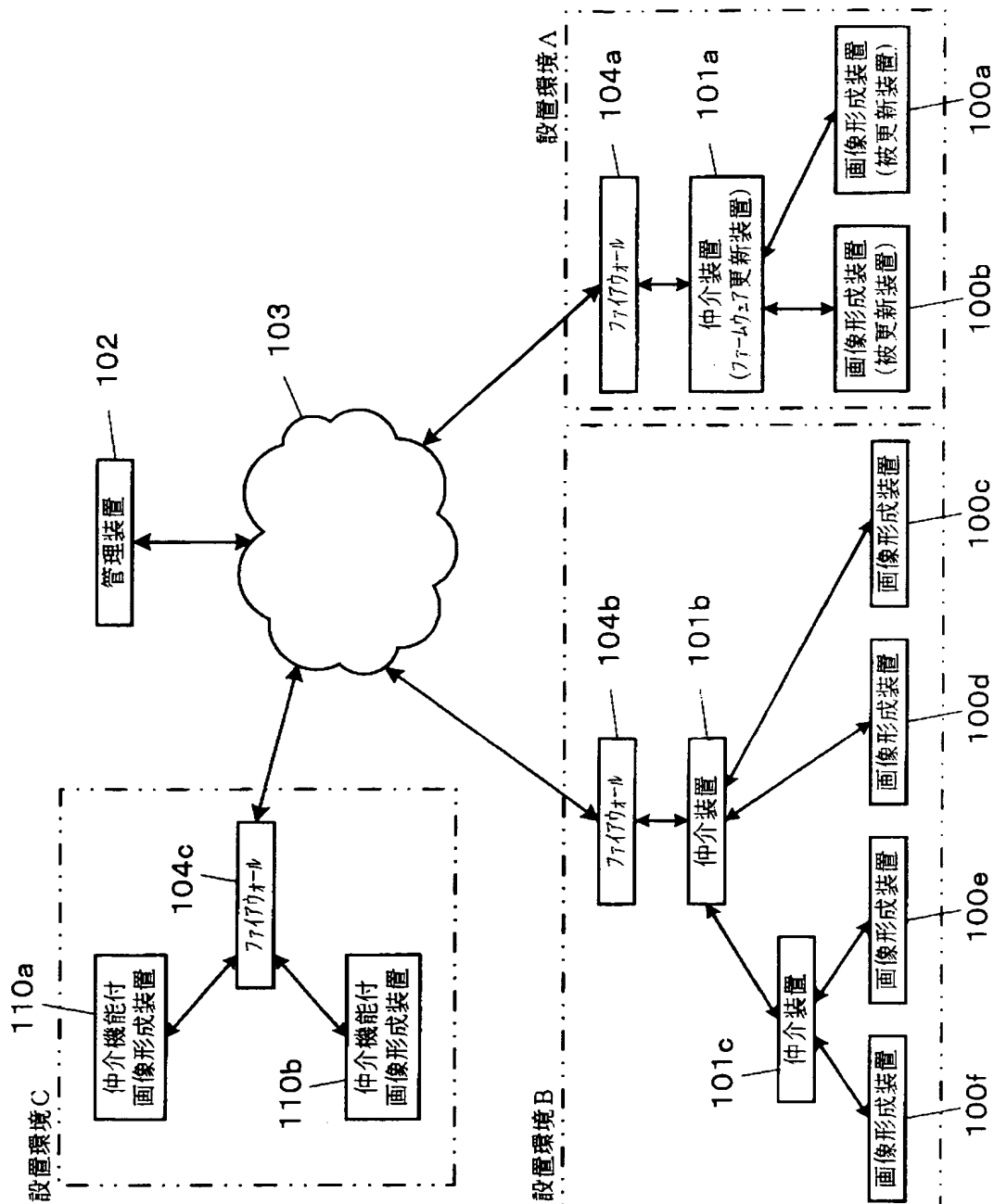
【図 3】



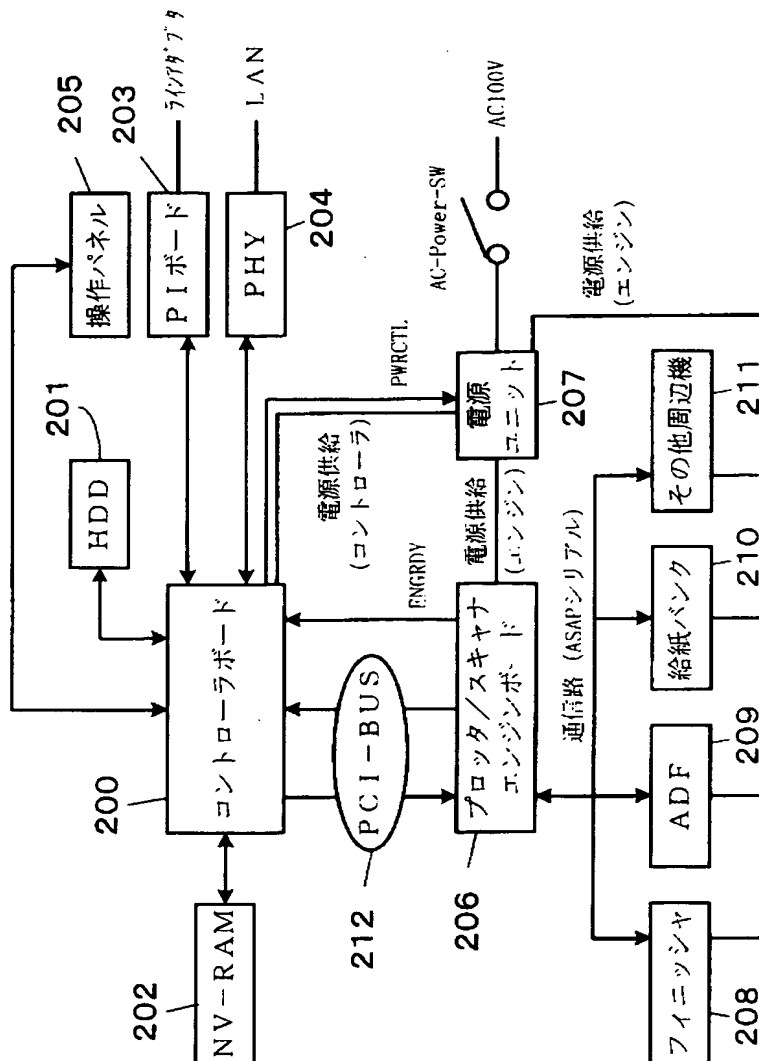
【図 4】



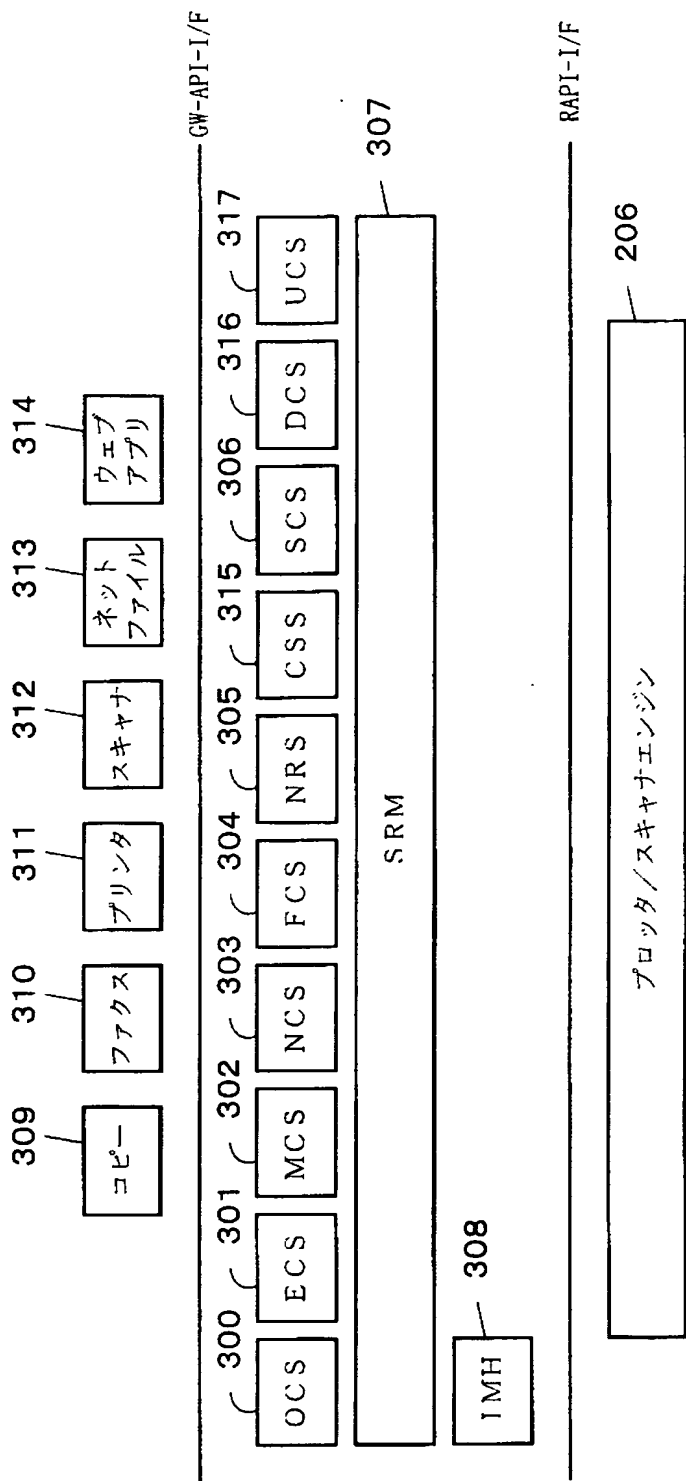
【図 5】



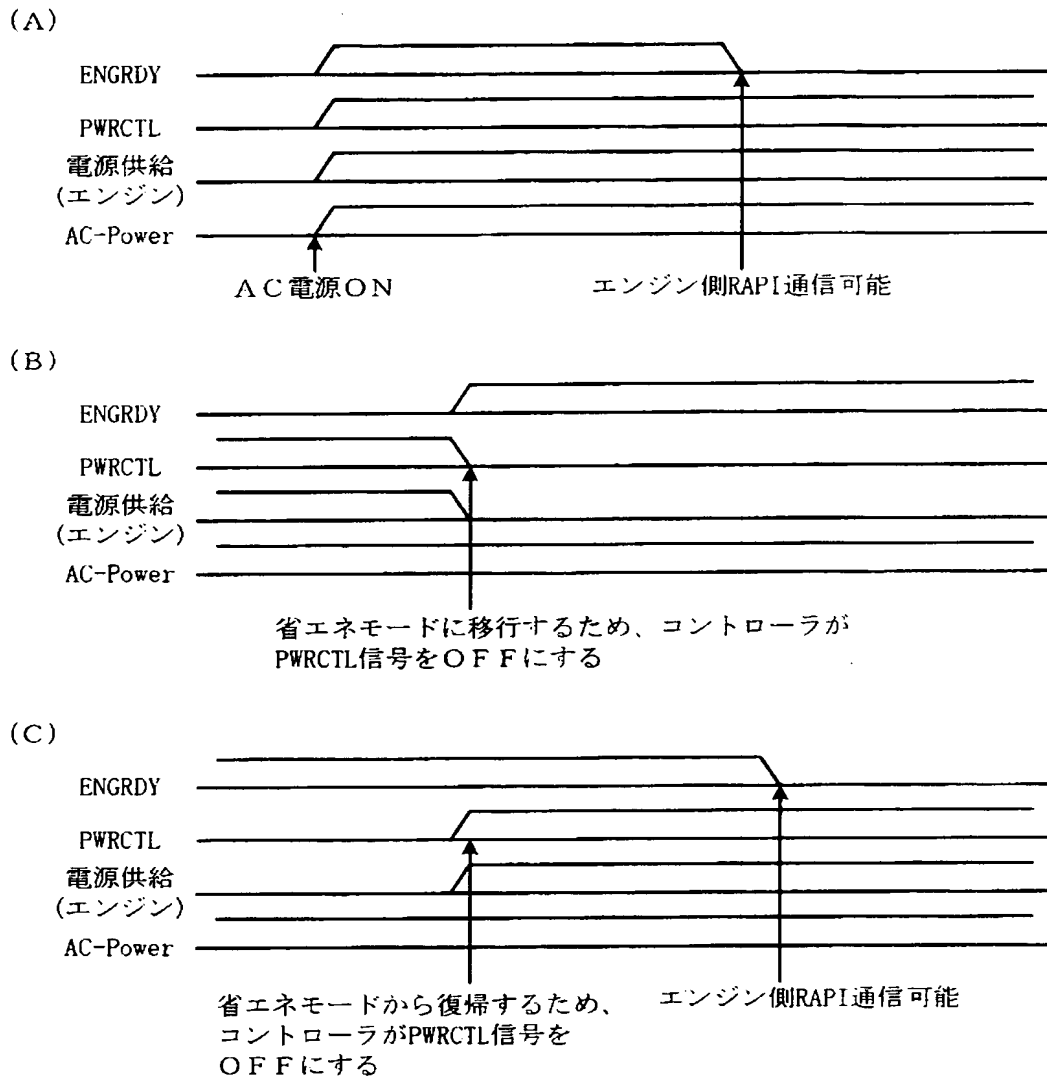
【図 6】



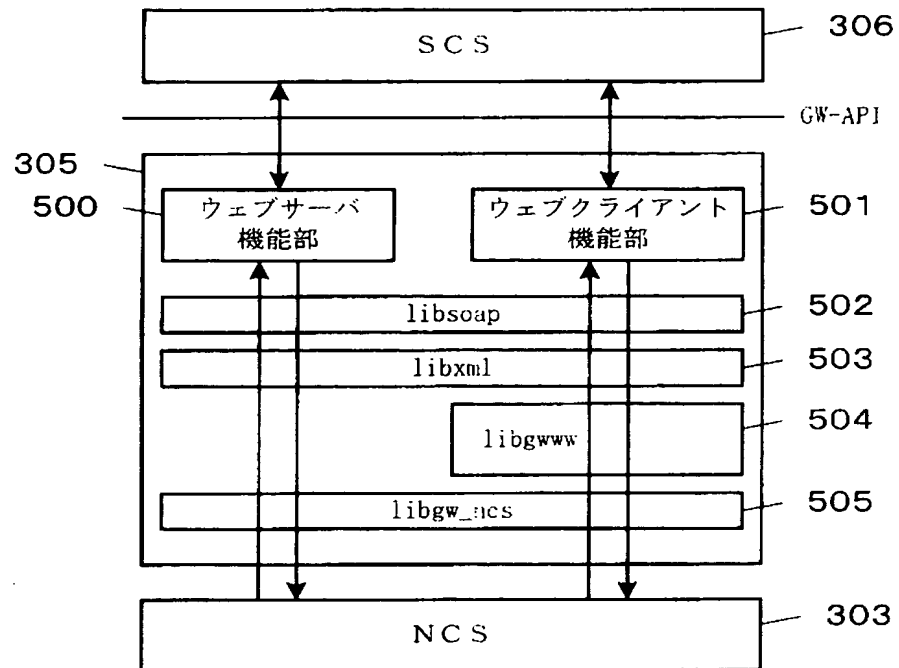
【図 7】



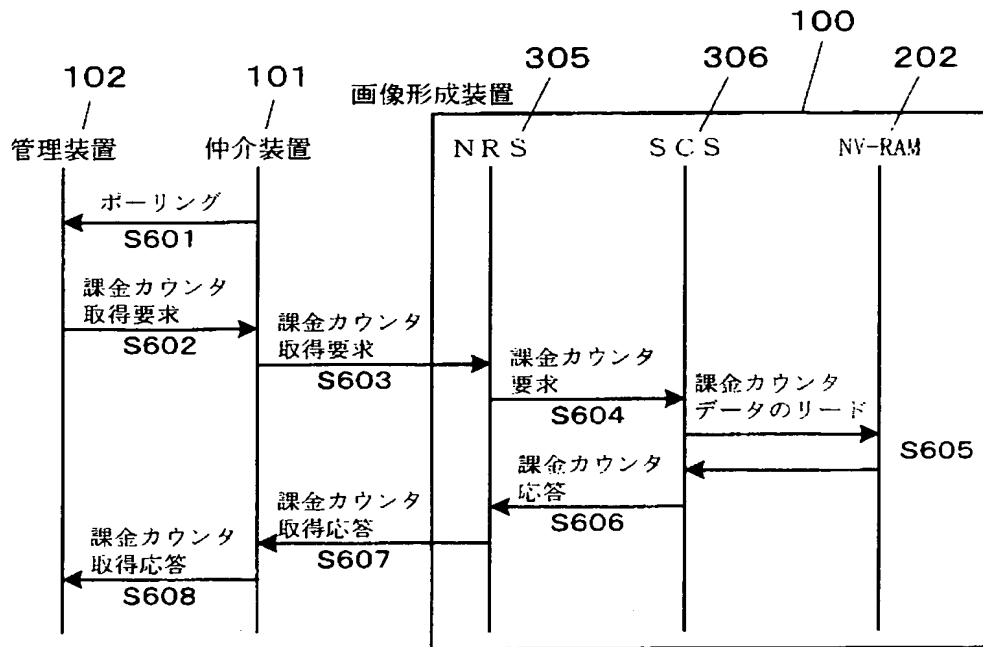
【図 8】



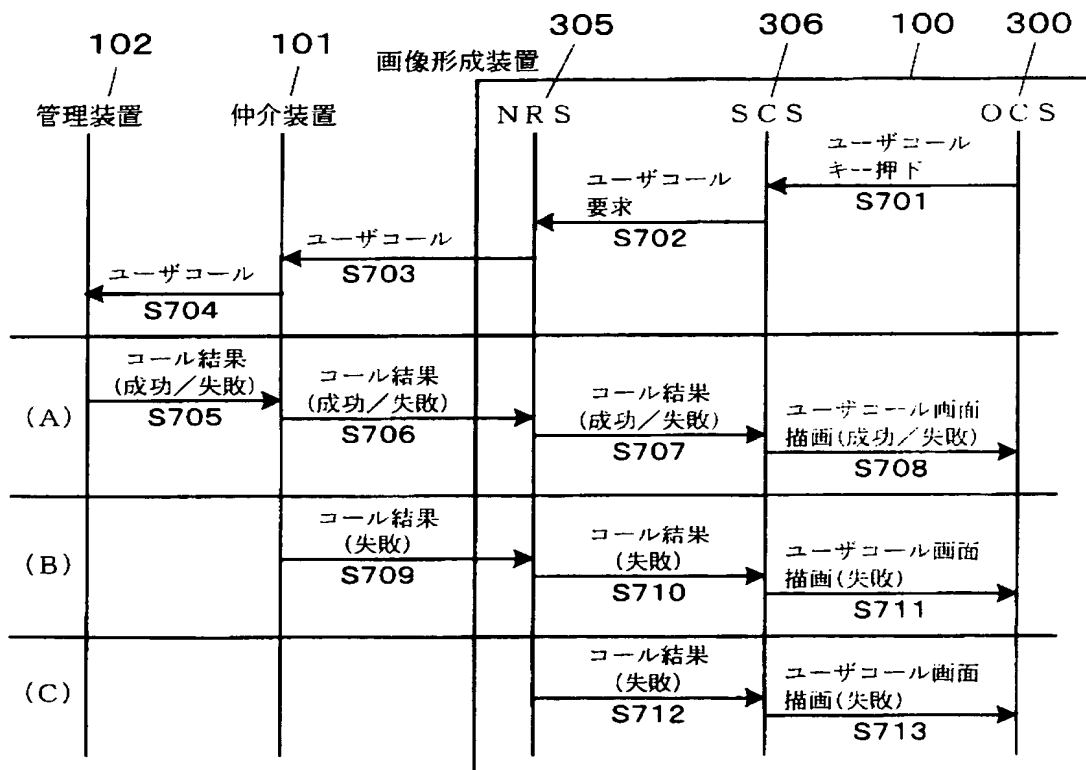
【図 9】



【図 10】



【図 11】



【図 12】

仲介装置側
(ファームウェア更新装置)

ルート鍵証明書
私有鍵 A
公開鍵証明書 A

仲介装置側処理

START

S21

接続要求を送信

S22

ルート鍵証明書を用いて公開鍵証明書 B の正当性を確認

S23

公開鍵 B で
第 1 の乱数を復号化

S24

第 2 の乱数と
第 3 の乱数を生成

S25

第 2 の乱数を私有鍵 A で、
第 3 の乱数を公開鍵 B で
暗号化

S26

暗号化した第 2、第 3 の
乱数と公開鍵
証明書 A を送信

S27

第 1、第 2、第 3 の乱数から
共通鍵を作成し、以後の
通信の暗号化に用いる

END

画像形成装置側
(被更新装置)

ルート鍵証明書
私有鍵 B
公開鍵証明書 B

画像形成装置側処理

START

S31

第 1 の乱数を生成し、
私有鍵 B で暗号化

S32

暗号化した第 1 の乱数と
公開鍵証明書 B を送信

S33

ルート鍵証明書を用いて
公開鍵証明書 A の
正当性を確認

S34

公開鍵 A で
第 2 の乱数を復号化

S35

私有鍵 B で
第 3 の乱数を復号化

S36

認証成功の応答を返す

S37

第 1、第 2、第 3 の乱数から
共通鍵を作成し、以後の
通信の暗号化に用いる

END

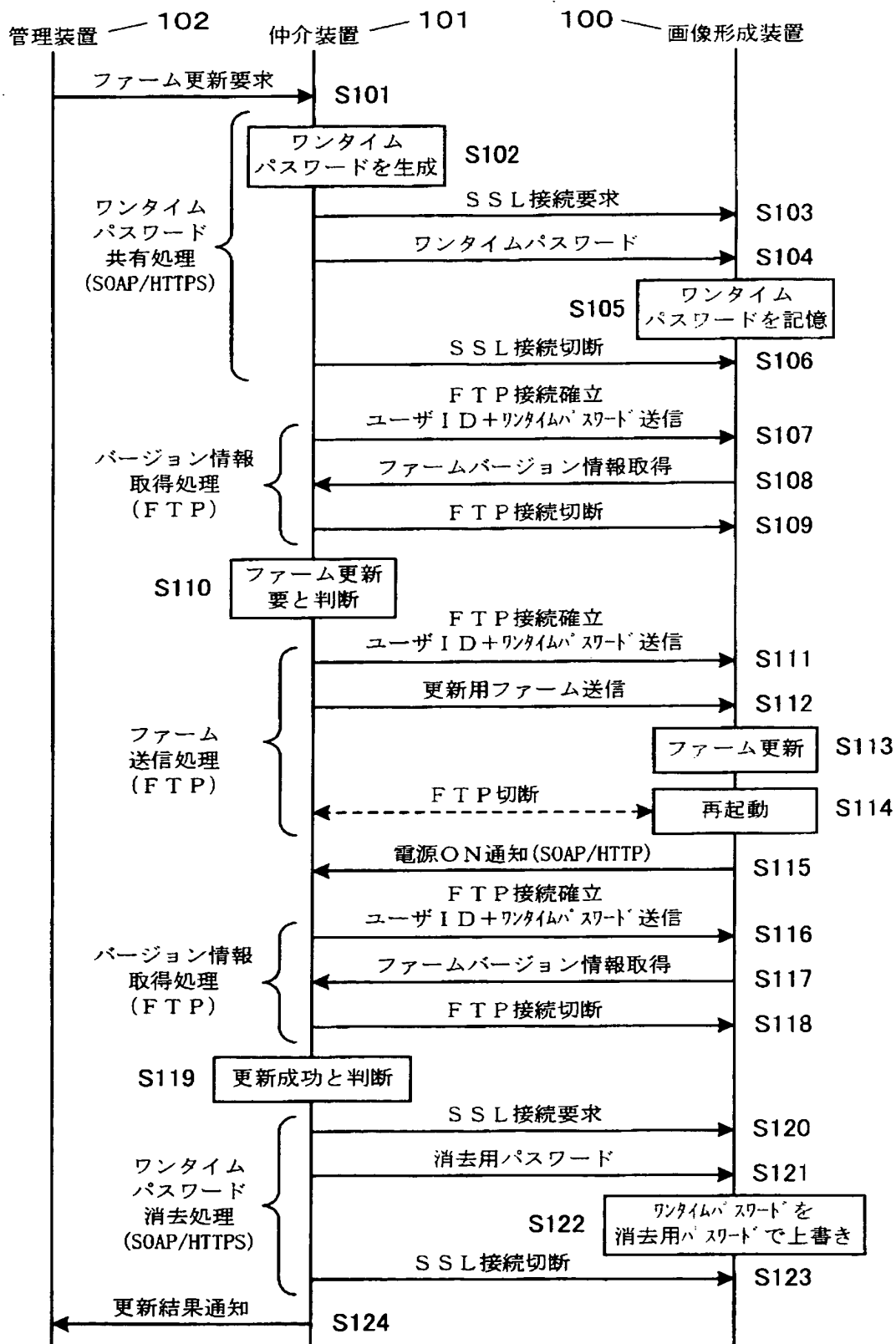
接続要求

第 1 の乱数 (暗号化) +
公開鍵証明書 B

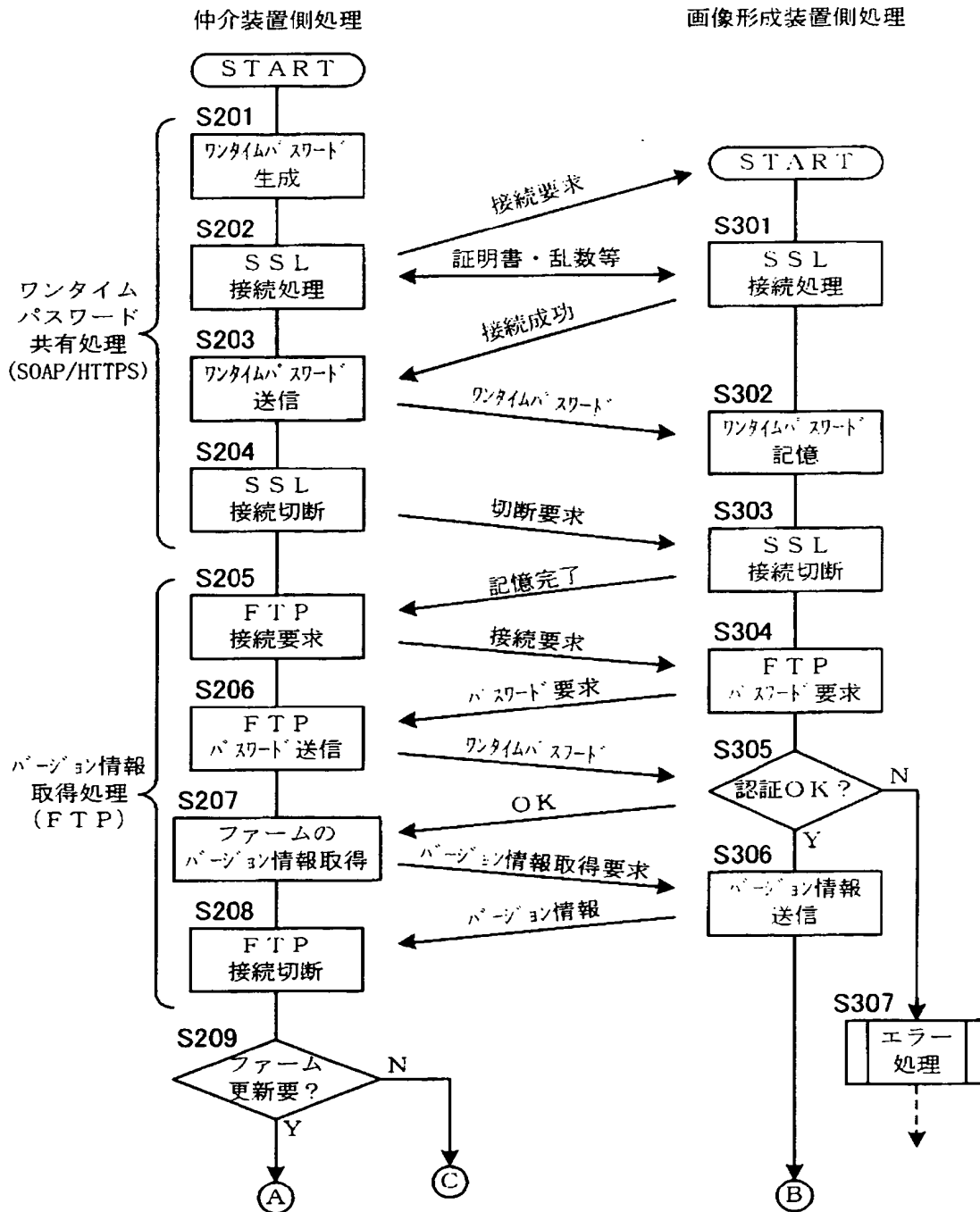
第 2、第 3 の乱数 (暗号化) +
公開鍵証明書 A

成功応答

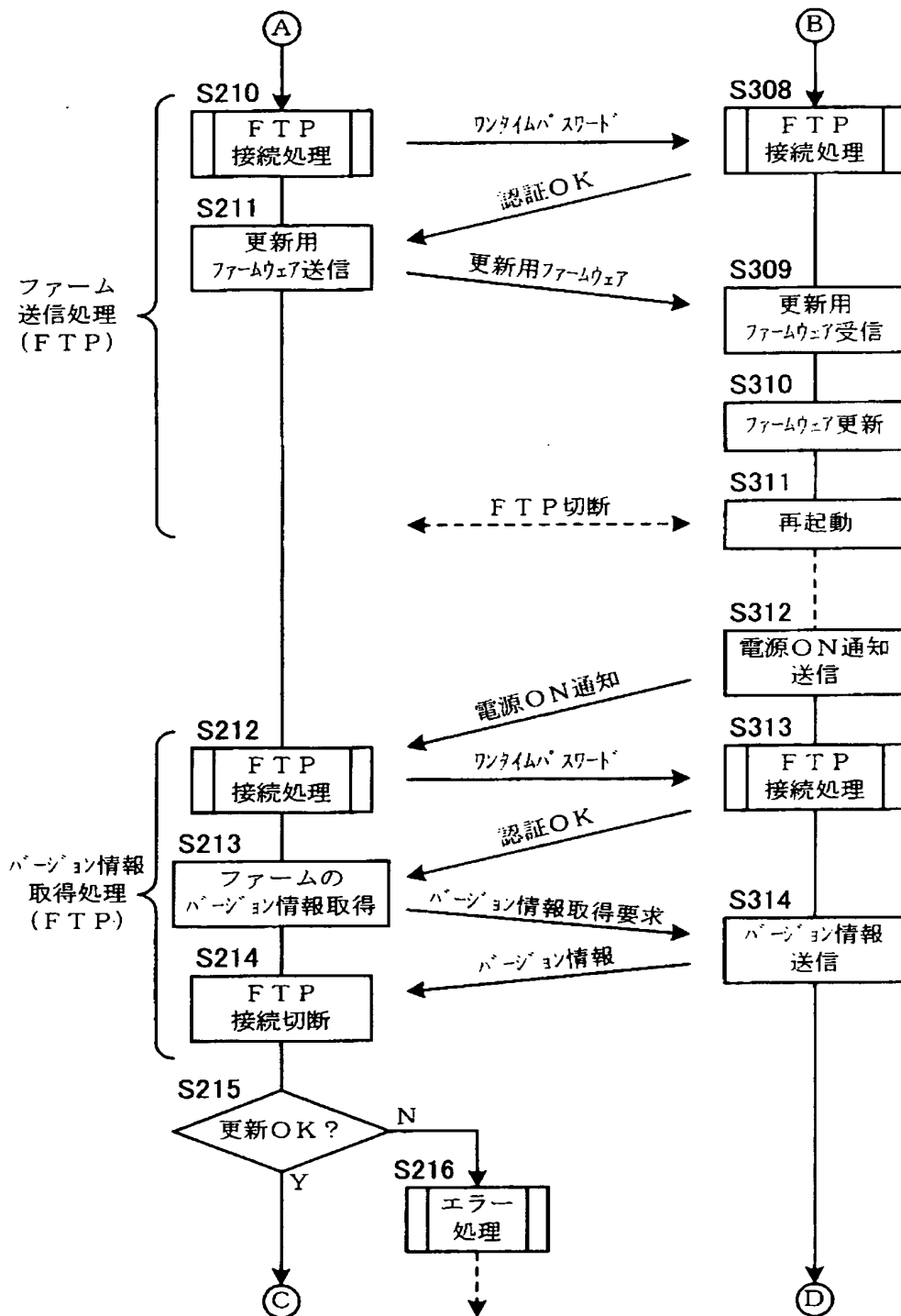
【図13】



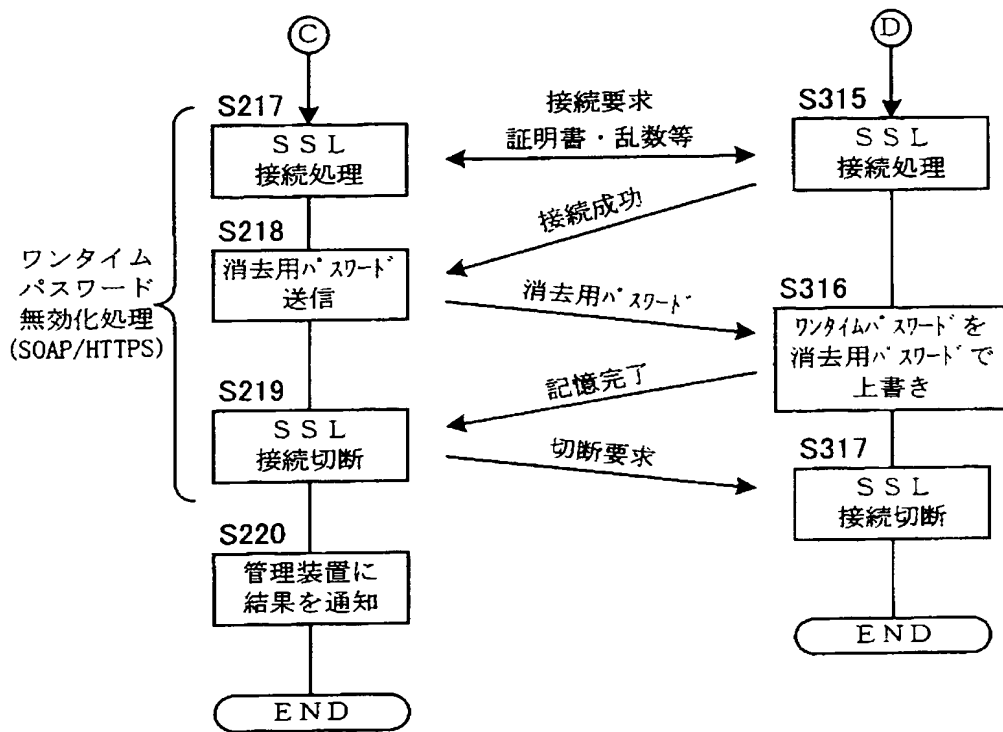
【図 14】



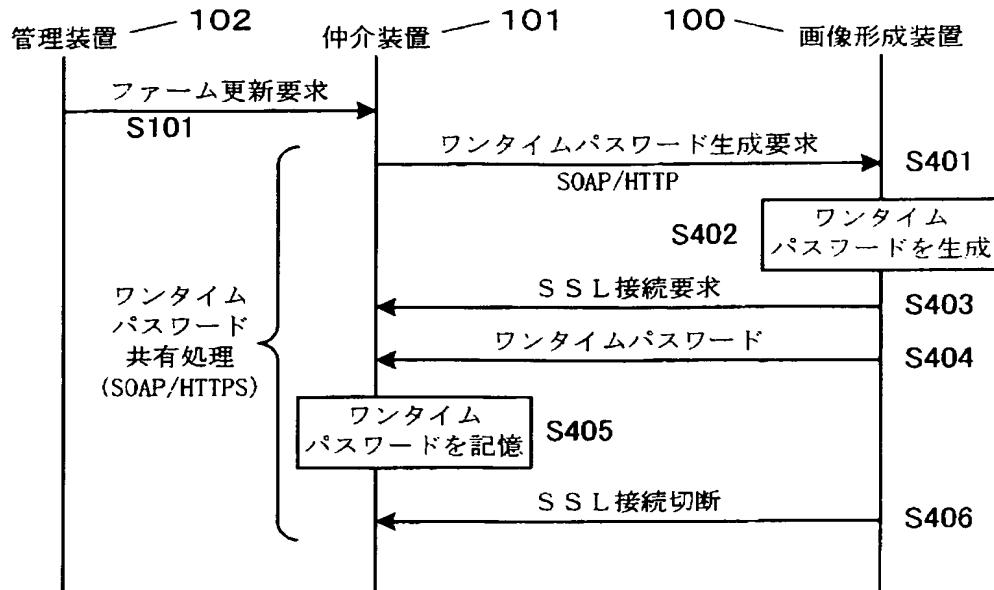
【図15】



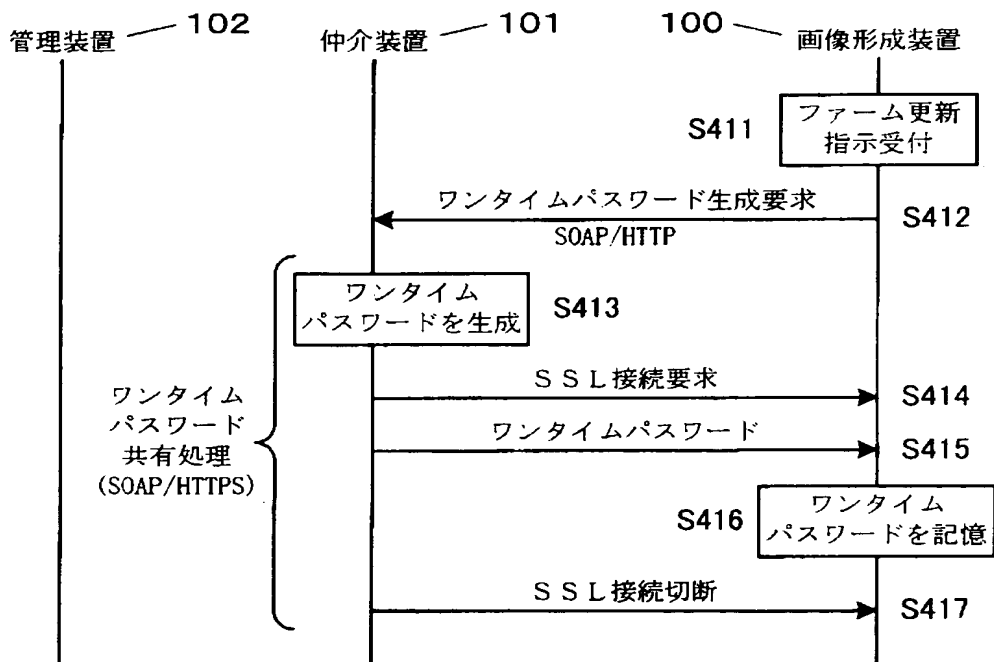
【図 16】



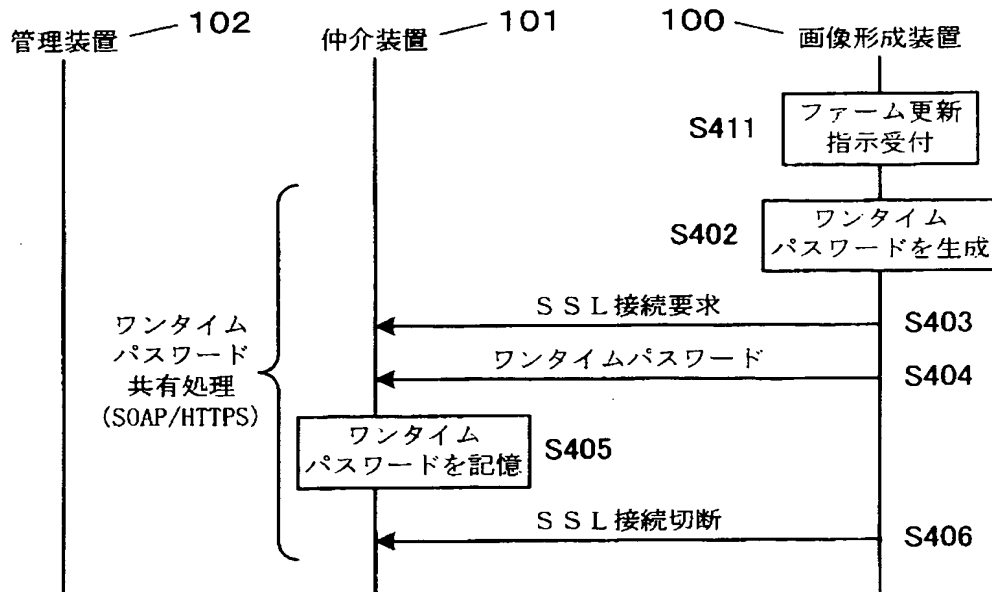
【図 17】



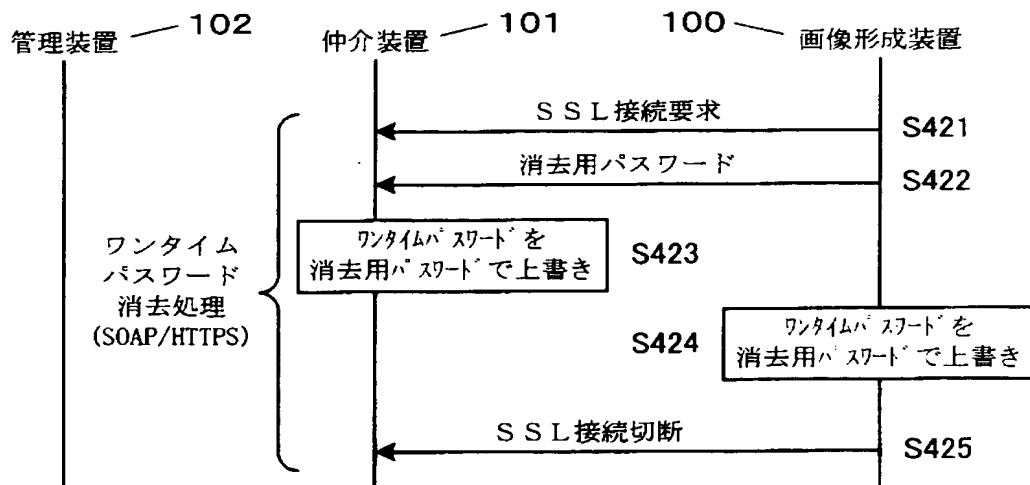
【図 18】



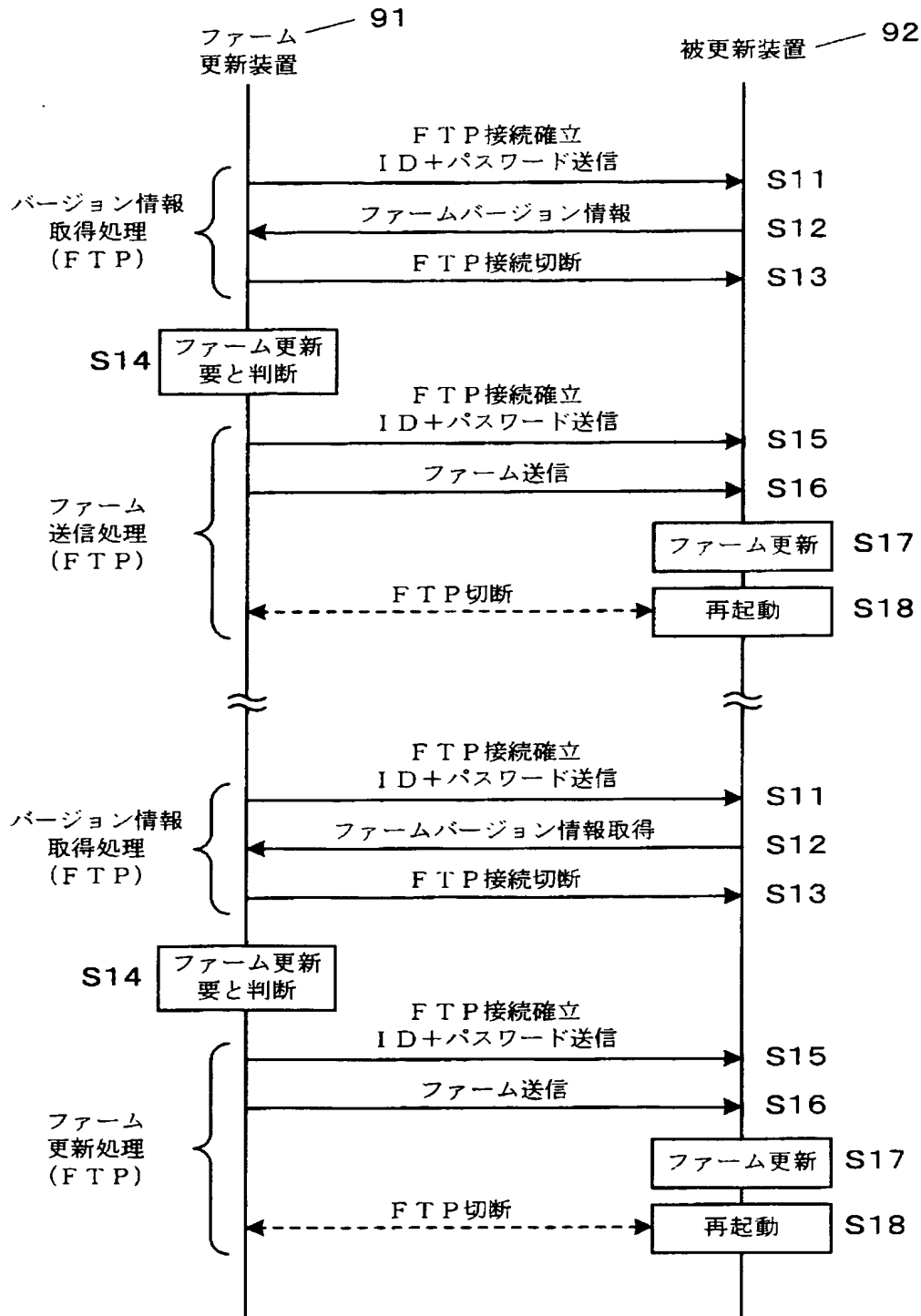
【図19】



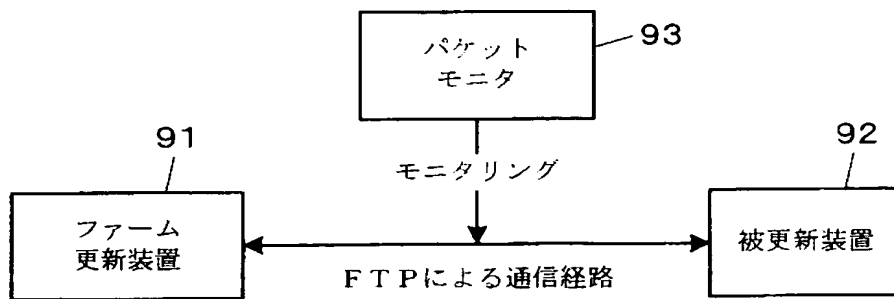
【図20】



【図 21】



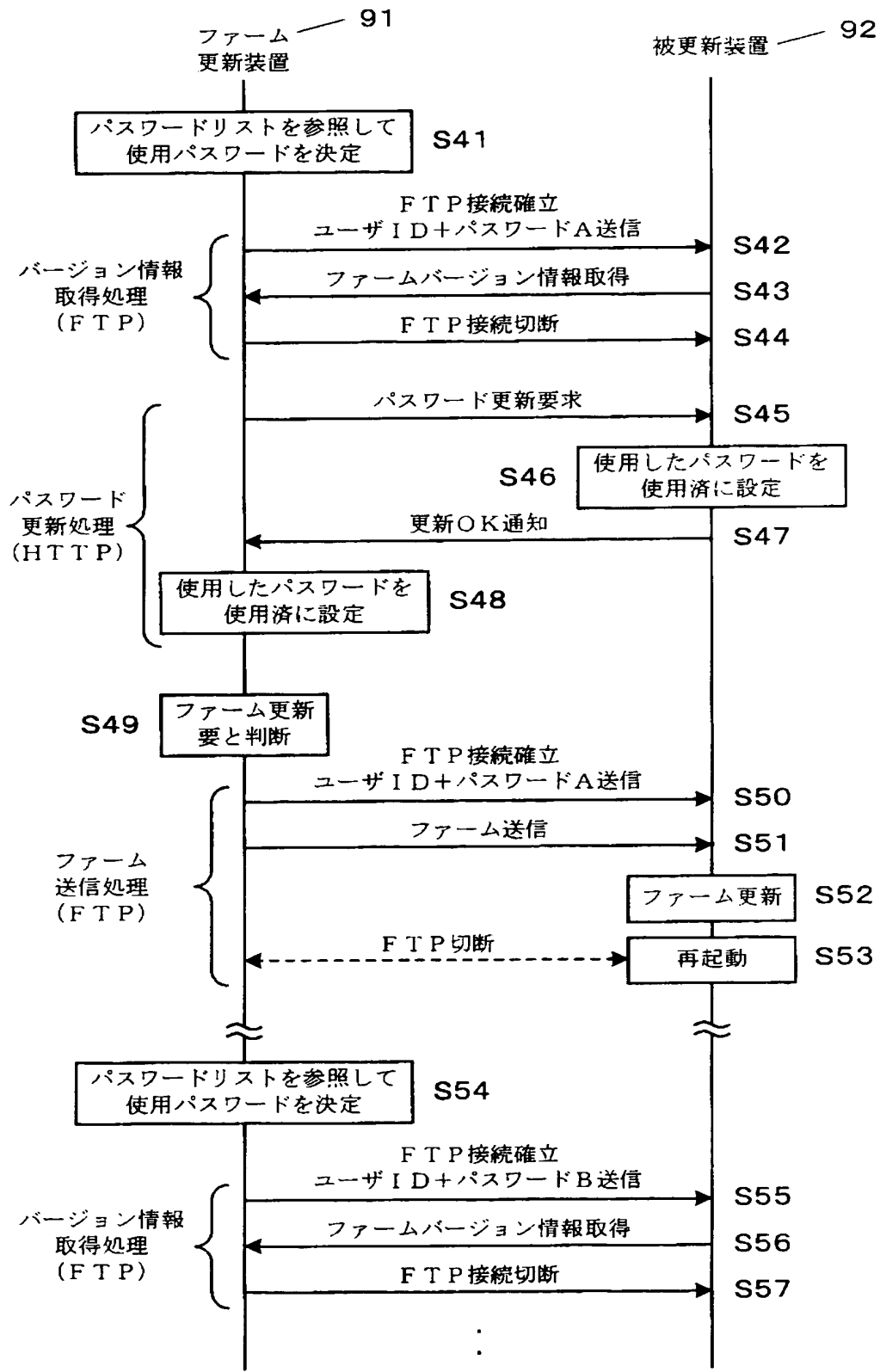
【図 2 2】



【図 2 3】

No.	使用済み／未使用	パスワード
A	使用済み	adfgjhuhgk
B	使用済み	hj75fgukja
C	未使用	5rhjdebha
⋮	⋮	⋮
X	未使用	rtgfc6qkqa
Y	未使用	6q3fgdysa

【図 24】



【書類名】 要約書

【要約】

【課題】 高い安全性を確保しながらコンパクトなソフトウェアによって更新処理を行うことができるようにする。

【解決手段】 ファームウェア更新装置（仲介装置101）によって、ネットワークを介して通信可能な被更新装置（画像形成装置100）のファームウェアを更新する場合において、仲介装置101がワンタイムパスワードを生成し、これをSSLを用いた通信経路で画像形成装置100に送信して記憶させ（S102～S106）、画像形成装置100にワンタイムパスワードをSSLよりも処理負荷の小さいFTPを用いた通信経路で送信して認証処理を行わせ（S111）、その認証処理が成功した場合に更新用ファームウェアをFTPによる通信経路で画像形成装置100に送信してファームウェアの更新を行わせる（S112, S113）。更新の成功が確認できた場合（S119）には、そのワンタイムパスワードを無効化するとよい（S120～S123）。

【選択図】 図13

特願 2 0 0 3 - 0 9 0 8 2 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー